ACCESS CONTROL STIG

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 1, Release 1

5 June 2006

Developed by DISA for the DoD

This page is intentionally left blank.

TABLE OF CONTENTS

Page

TABLE OF FIGURES

TABLE OF TABLES

This page is intentionally left blank.

1. INTRODUCTION

1.1 Background

This Access Control Security Technical Implementation Guide (STIG) details a security framework for use when planning and selecting access control for protecting sensitive and classified information in the Department of Defense (DoD). It provides a consolidated starting place for the security planning team responsible for ensuring compliance with DoD policies. This STIG presents a practical methodology for selecting and integrating logical and physical authentication techniques while tying the solution to the asset's value, environment, threat conditions and operational constraints. For classified access, the solution must protect access to sensitive or classified systems and data while considering the need for appropriate and authorized access in uncontrolled areas for DoD personnel, contractors, and coalition forces.

Homeland Security Presidential Directive (HSPD) 12 seeks to address the problem of inconsistent and potentially insecure forms of identification that have been used to access Federal buildings and information systems. The National Institute of Standards and Technology (NIST) released a new standard called Federal Information Processing Standards (FIPS) 201, which provides guidance for implementation of HSPD12. HSPD12 will require federal government agencies to authenticate users at network, system, application, and desktop levels to a minimal degree of authentication assurance.

Once users authenticate themselves, however, they often find that they are required to do it again for each new resource they wish to access. This is inconvenient, especially if different passwords are required for each application. The DoD solution is the deployment of a standardized identity and access management solution within the DoD Public Key Infrastructure (PKI) architecture in conjunction with a cryptographic smartcard token know as the Common Access Card (CAC). This solution, once completely implemented across DoD, will enable users to access multiple applications in a single session after having been successfully authenticated and a digital identity established at a single logical access control point.

Access control is key to the protection of DoD physical and logical assets. Access control has several critical components; identity proofing, credential production, personalization, issuance, authentication of identity, permissions authorization, hardware and software switch control, transaction logging, and nonrepudiation. This STIG is focused on technologies and techniques employed to support authentication of identity. This guidance supports DoD's implementation of the Government's mandate to provide appropriate levels of assurance when verifying the identity of individuals seeking physical and electronic access to federally controlled facilities and information systems.

Although this document provides background information on physical security authentication methods, policies for implementation of physical security techniques are outside the scope of this document. Security Managers should reference the appropriate policy guidance for specific policies when implementing these physical security techniques as part of the access control solution. This document provides a perspective on how information technology solutions can be used either in place of or in combination with physical security techniques to provide appropriate protection for DoD assets.

Section 2 provides an overview of access control terms and introduces the layered approach required when planning and implementing access control solutions. Section 3 gives an overview of the methods and technologies used for asset protection and provide guidance and policies for implementation. Section 4 describes the methodology and considerations for selecting appropriate access control solutions by providing recommended steps and a table showing options available given particular asset values.

1.2 Authority

DoD Directive 8500.1 requires that "all IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved security configuration guidelines" and tasks DISA to "develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA." This document is provided under the authority of DoD Directive 8500.1.

This document also provides supplementary information and guidance for IAOs and other responsible Security Managers regarding physical access controls. This guidance is consistent with the policies of DOD 5200.1-R and 5200.8-R. This information is provided in support of the stated purpose of the Access Control STIG, which is to facilitate the integration of logical and physical security controls in protecting IA and IA –enable IT products.

The use of the principles and guidelines in this STIG will provide an environment that meets or exceeds the security requirements of DoD systems operating at the Mission Assurance Category (MAC) II Sensitive level, containing sensitive information.

1.3 Scope

This document is a requirement for all DoD administered systems and all systems connected to DoD networks. These requirements are designed to assist Security Managers, Information Assurance Managers (IAMs), Information Assurance Officers (IAOs), and System Administrators (SAs) with configuring and maintaining security controls. This guidance supports DoD system design, development, implementation, certification, and accreditation efforts.

Intenerated security solutions are often best if designed by a multi-disciplined team. This security design team should consist of representatives from any or all of the following areas:

- The data owner or designated representative
- The IAO or responsible physical Security Manager
- Host installation security representatives
- GSA representative (if the facility is GSA-owned
- Civilian police officials, as applicable

1.4 Writing Conventions

Throughout this document, statements are written using words such as "**will**" and "**should**." The following paragraphs are intended to clarify how these STIG statements are to be interpreted.

A reference that uses "**will**" implies mandatory compliance. All requirements of this kind will also be documented in the italicized policy statements in bullet format, which follow the topic paragraph. This will make all "**will**" statements easier to locate and interpret from the context of the topic. The IAO will adhere to the instruction as written. Only an extension issued by the Designated Approving Authority (DAA) will table this requirement. The extension will normally have an expiration date, and does not relieve the IAO from continuing their efforts to satisfy the requirement.

A reference to "**should**" is considered a recommendation that further enhances the security posture of the site. These recommended actions will be documented in the text paragraphs but not in the italicized policy bullets. Nevertheless, all reasonable attempts to meet this criterion will be made.

For each italicized policy bullet, the text will be preceded by parentheses containing the STIG Identifier (STIGID), which corresponds to an item on the checklist and the severity code of the bulleted item. An example of this will be as follows: "(*G111: CAT II*)." If the item presently has no STIGID, or the STIGID is being developed, it will contain a preliminary severity code and "N/A" (i.e., "*[N/A: CAT III]*").

1.5 Vulnerability Severity Code Definitions

Severity (CAT) Codes are a measure of risk used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Code (CAT) of CAT I, II, or III. Each policy is evaluated based on the probability of a realized threat occurring and the expected loss associated with an attack exploiting the resulting vulnerability.

For access control, policies are classified as CAT I if failure to comply may lead to an exploitation which: has a high probability of occurring; does not require specialized expertise or resources; and leads to unauthorized access to high value information (e.g., Classified). Exploitation of CAT I vulnerabilities allow an attacker physical or logical access to a protected asset, allows privileged access, bypasses the access control system, or allows access to high value assets (e.g., Classified). CAT I vulnerability include allowing access to the access control system administrative password, failure to identity proof prior to badge issuance.

Exploitation of CAT II vulnerabilities also leads to unauthorized access to high value information; however, additional sophistication, information, or multiple exploitations are needed. Exploitation of CAT II vulnerabilities provides information that have a high potential of allowing access to an intruder but requires one or more of the following: exploitation of additional vulnerabilities; exceptional sophistication or expertise; or does not provide direct or indirect access to high value information (e.g., Classified). Examples: Users are not trained to protect the CAC and PIN.

An access control policy with a CAT III severity code requires unusual expertise, additional information, multiple exploitations, and does not directly or indirectly result in access to high value information. Exploitation of CAT III vulnerabilities provide information that potentially could lead to compromise but requires additional information or multiple exploitations, but does not provide direct or indirect access to high value information. Example: Failure to review audit logs regularly.

Exploitation of CAT IV vulnerabilities, when resolved, will prevent the possibility of degraded security. Does not provide direct or indirect access to high value information

NOTE: Category IV may be eliminated in future DoD policy, thus this category is not used in this STIG.

Vulnerability Severity Codes	
Category I	Vulnerabilities that allow an attacker immediate access into a machine, allow superuser access, or bypass a firewall.
Category II	Vulnerabilities that provide information that have a high potential of giving access to an intruder.
Category III	Vulnerabilities that provide information that potentially could lead to compromise.
Category IV	Vulnerabilities, when resolved, will prevent the possibility of degraded security.

Table 1-1. Vulnerability Severity Code Definitions

1.6 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site located at http://iase.disa.mil. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information.

1.7 Document Revisions

Comments or proposed revisions to this document should be sent via e-mail to **fso_spt@disa.mil**. DISA Field Security Operations (FSO) will coordinate all change requests with the relevant DoD organizations before inclusion in this document.

2. ACCESS CONTROL LAYERS

An access control method protects systems, resources, or information assets by allowing authorized access and/or detecting and deterring unauthorized access. Some access control methods may also validate the level of authorization or need-to-know for an authenticated user. Assets can be physical or logical. Physical assets may include items such as classified written material, buildings, equipment, or personnel. Logical assets may include items such as intellectual property or electronically stored privacy act and sensitive or classified data.

An effective security solution proactively implements access control methods using a holistic rather than a reactive, bit-by-bit approach. The solution should leverage information about the asset and its environment and provide defense-in-depth (also known as security-in-depth) using layered security techniques. This layered approach calls for an integrated solution combining complementary security controls at a sufficient level to deter and detect unauthorized entry and activity within the facility or logical system. Figure 2-1, Layered Protection of Assets, illustrates the concept of a layered or security-in-depth approach for the protection of an asset. Note that not all asset environments will have every layer, as explained in subsequent sections of this document.

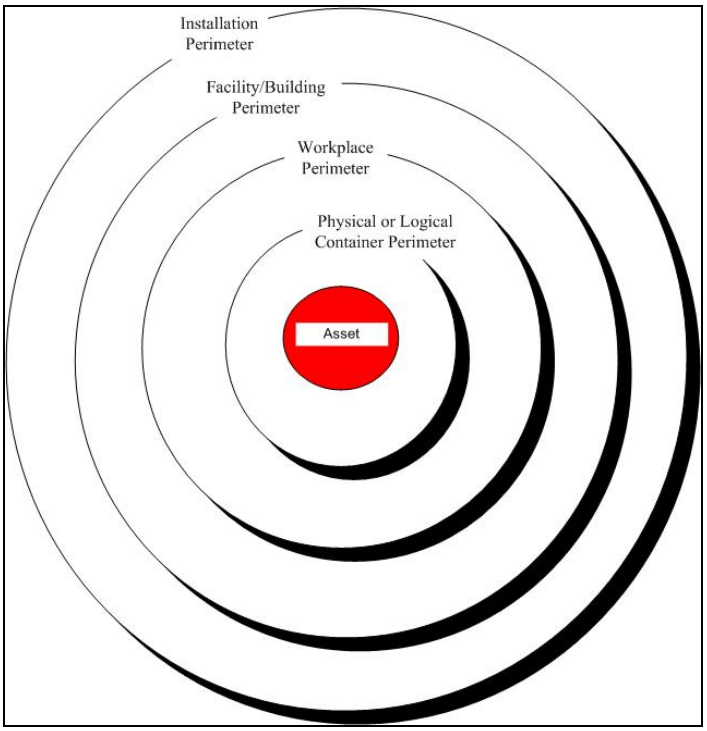

Figure 2-1. Layered Protection of Assets

Since it is impossible to design the perfect security solution at each layer, gaps or vulnerabilities for each layer are mitigated by the strengths at subsequent layers. Confidence in the access control system increases with the use of multiple access control techniques used together or at various layers or perimeters of the access process and when the methods offering greatest personal authentication assurance are closest to the asset being protected.

Threats to assets stem from two general categories: catastrophic events such as natural disasters and events caused by humans. The catastrophic threat is not the main focus of this document but is very important when planning for business continuity. The threat to assets from adverse human behavior can come from an insider or outsider. Thus, allowing authorized access must include methods for: identification, authentication, authorization, and auditing. These steps will result in a robust solution with an appropriate level of assurance that the system is accessed by authorized users who have a validated need-to-know.

Access control must include detection and initial response to (i.e., denial of entry) unauthorized individuals. These procedures detail what happens when unauthorized access is detected or is successful. A disaster recovery plan must be in place to ensure mission continuity and recovery. Procedures for incident handling must include process improvement.

The same process of determining assets, risk levels, and applying the security framework applies to both tactical and non-tactical environments. Identifying potential threats and the level of protection required for the assets are necessary. Commanders must also identify additional vulnerabilities, which are unique to the specific tactical environment and mitigate these risks.

2.1 The Access Control Perimeter

An access control perimeter is a layer of physical or technical elements used to permit or deny access to or from a restricted area or system. An access control point (ACP) is the point where users are either allowed or denied access. A perimeter may have multiple ACPs, each point should be controlled using appropriate methods as discussed in later sections of the document.

Figure 2-1, Layered Protection of Assets, depicts the layers applicable to the DoD environment. However, not all layers are present or relevant for all assets. Asset protection must start with an evaluation of the asset being protected and build outward from the asset. The Security Manager must assess the environment inside and outside the asset container, i.e., the Physical or Logical Container Perimeter. The purpose of the access control system must be clearly defined with respect to the asset being protected. An assessment of the assets value, type, and the known tactics, which may be used to gain unauthorized access or damage the asset, is an important step. Another challenge is the determination of where the outermost access control perimeter must be placed. This decision is based upon DoD policy governing the protection of the specific type and value of an asset as discussed in subsequent sections.

The outer access control perimeter is the physical or logical point where users first encounter access control. This layer is commonly referred to as simply “the perimeter”. This outer perimeter can occur at any point in the security layer depicted in Figure 2-1 and is determined by a multi-disciplined team as described in Section 1.3.

Using the access control security framework, the security team can appropriately combine and implement security techniques at the ACPs of the Asset Container Layer and the ACP of the outer access control perimeter. Figure 2-2, shows a fixed-base example of the various points where security could be implemented using the layered approach depicted in Figure 2-1.

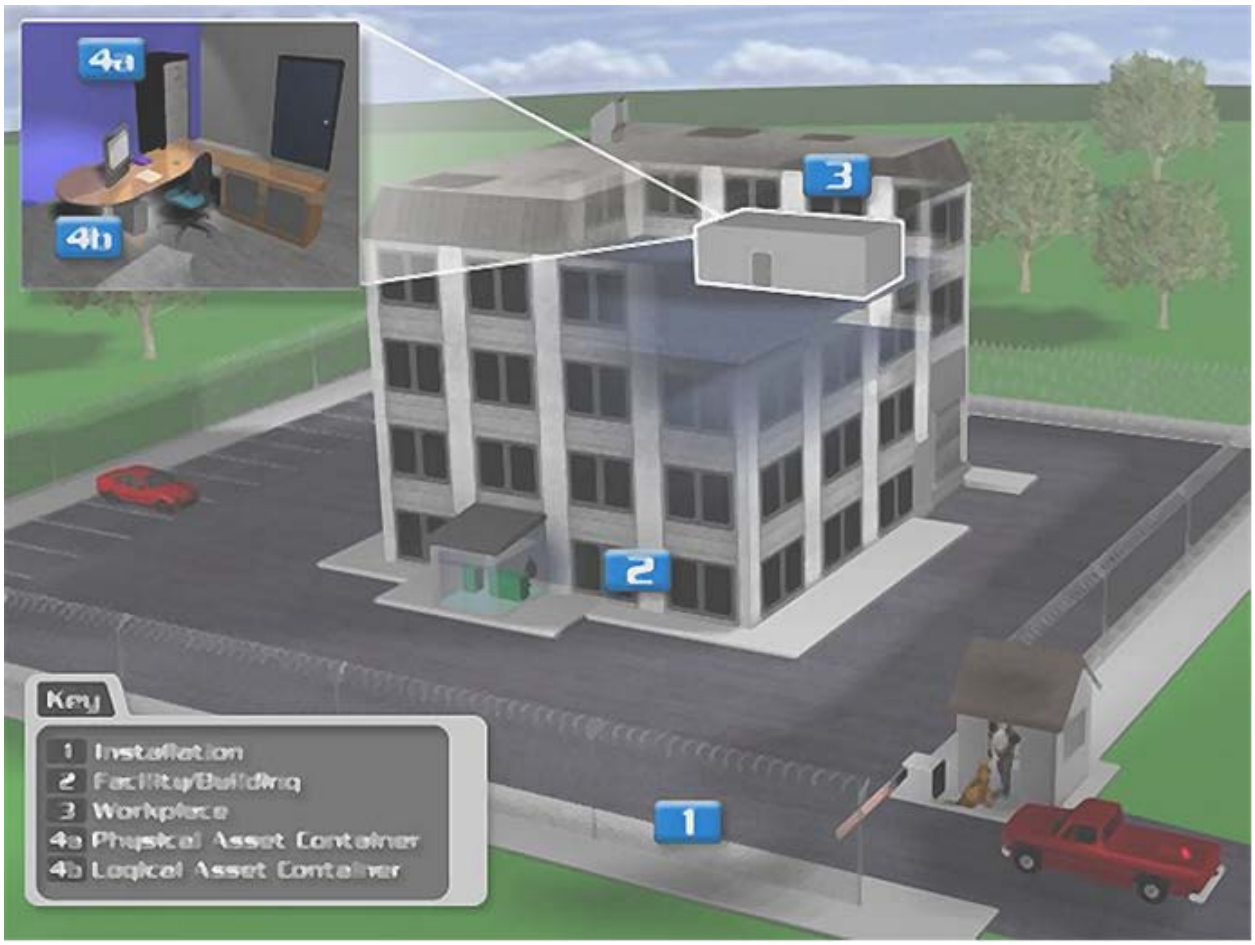

Figure 2-2. Potential Access Control Perimeters

The following subsections define each security layer and outlines potential issues and considerations for each layer. Special issues relating to selection of the layer as the outermost access control perimeter are also highlighted.

2.1.1 Asset Container Perimeter

An asset container is the physical or logical location of a resource. Figure 2-2, items 4a and 4b are two examples of common asset containers, a safe and a computer/network. The asset container perimeter is the first point of the container where the user encounters asset controls. Controls at this layer are the most stringent as this is the layer closest to the asset.

NOTE: The outermost access control perimeter will be located at this level for physical assets protected by a safe or secure container. This is also the innermost access control perimeter for gaining access to logical assets through use of remote or wireless connection methods.

Physical asset containers such as safes, vaults and Sensitive Compartmented Information Facilities (SCIFs) are used at this layer to protect classified material and equipment. Classified materials must also be properly marked, tracked using a log, and transported using the proper

cover sheets and envelopes as required by DoD policy. Security guards, automated entry biometric systems, smart cards, memory cards, badges, tokens, and other forms of access control methods can be combined at this perimeter to control and monitor access. Deterrents such as posted signage and alarms can also be used. Proper checklists and periodic inspections are required by DoD policy.

Logical asset containers include networks such as Secret Internet Protocol Router Network (SIPRNet) or Non-Classified (but Sensitive) Internet Protocol (NIPRNet) Enclaves. DODD 8500.1 defines the Enclave as a "collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security". Securing this asset container perimeter requires access control methods protecting:

- The Enclave perimeter
- The data and communications while in transit and at rest
- Applications (e.g., office automation, web servers, and email)
- Databases
- Server, host, or client device (wired, wireless, and remote)

Protective methods used to protect this layer include: administrative policies; physical policies such as locks, safes or SCIFs; architecture components such as firewalls and Network Intrusion Detection Systems (IDSs); passwords and tokens; biometric systems, encryption, auditing, and training. The primary sources for policies applicable to the logical perimeter are DODI 8500.2 and the applicable DoD STIGs. These documents provide standards for protecting data at rest and in transit, user authorization, and required administrative controls needed for protecting DoD logical assets. The primary source for policies applicable to the physical perimeter is DoD 5200.8-R.

NOTE: If a logical asset perimeter is contained within a SCIF (or physical container) then the data container is the perimeter closest to the asset, i.e., the logical container.

2.1.1.1 Wireless and Remote Computing

Wireless and remote computing usually bypass the outer physical layers of the access control framework. The user enters the logical Asset Container Layer and requests access to the Enclave. This is problematic as the additional assurance provided by other layers is not present. In this case the access control perimeter and the data container perimeter are the same. Multi-factor access control methods, discussed in later sections of this document, are indicated to support wireless and remote computing. Careful combination of the proper methods is particularly critical when protecting high value (i.e., sensitive or classified) assets.

2.1.2 Workplace Perimeter

The workplace can be a single room, suite, or area on one or multiple floors of a building or installation. Figure 2-2, item 3 depicts one example of commonly used workplace layer, an office in a multistory building. The workplace layer is most frequently used as the access control perimeter in DoD facilities and installations. This is because workplaces are typically smaller,

defined areas that lend themselves to effective controlled access implementations. If a workplace is an open storage area for classified materials, the asset container perimeter and the workplace perimeter are the same and stringent methods must be used for perimeter controls.

To protect the workplace perimeter, the ACPs must be identified and secured. Potential access points such as elevators, stairways, windows, doors, and walls must be considered. Also consider ventilation, plumbing, electrical ductwork, and drop-tile ceilings when guarding against adversarial access. Workplaces located in a mid-level floor at least 18 to 20 feet from the ground or below roof level provide a more easily secured environment than a ground level or top floor room.

In many environments, individuals without the required need-to-know may enter a building but must remain outside of the workspace perimeter. Gardeners, maintenance contractors, and delivery people may be allowed access at the building perimeter but blocked at the workspace perimeter. In this case, the building perimeter is not part of the asset's access control environment. A guard or attendant, who is trained to identity proof visitors in accordance with DoD policies and subsequent sections of this document, should be used in workplaces with frequent visitors. In many cases, both automated systems and manual systems are used, where the automated systems support those who routinely work in the protected area and the receptionist or guard supports visitor access processing.

Tracking both entry and exit of authorized users should be considered to circumvent possible use of copied or fake access control credentials. This type of tracking can detect use of credentials already used for entry but not yet used for exit (i.e., the authorized individual is already within the building). Conversely, if the adversary entered first and the authorized individual was denied access, the security guard could be alerted to search for the imposter.

2.1.2.1 Open and Closed Storage

Unless the workspace has open storage, classified physical assets must be in the custody of an authorized individual at all times and must be returned to the GSA-approved container or destroyed when the need for access is no longer required. If the workspace is not configured to support open storage of classified assets, procedures for proper storage of such assets must be defined and employed IAW DoD 5200.1-R, Information Security Program or the Target of Evaluation (TOE) Security Policy.

2.1.3 Facility/Building Perimeter

A facility is any single building, project, or site. Figure 2-2, item 2 depicts one example of a commonly used facility/building perimeter, a guarded building entryway. Note that the loading dock at the side of the building must also be secured. The facility/building perimeter may also be designated as the asset's access control perimeter. Government assets are housed in both commercial and government-owned or leased buildings. Consider the building depicted in Figure 2-2. This building has many ACPs to be considered. Main entrances and exits, emergency exits, windows, fire escapes, loading docks, roof accesses, sewer access, and connected parking garages. Often, only a subset of the individuals requiring access to the building or facility perimeter are authorized for access to specific assets protected within the

facility. Additional identity proofing will be required closer to the protected asset to ensure that authorization and permissions are verified before access is granted.

Security Managers should use the results of the risk assessment (as defined in later sections), to validate the need for implementing access controls at this layer in order to avoid overprotecting the asset. If the building requires frequent access by visitors, other workers in the building, maintenance staff, gardeners, delivery persons, consider the cost and complexity of implementing the required controls. If the need is valid, entry procedures for these temporary workers and also for emergency personnel are needed. If the perimeter can be established at the building layer, the level and complexity of the building internal area controls can be diminished without negatively affecting security assurance of the asset(s) being protected. On the other hand, if it is not practical to establish a perimeter at the building or facility layer, the Security Manager or Team should attempt to establish the access control perimeter as far as practical from any classified operations or assets within the building (e.g., at a controlled workspace within the building as described above).

2.1.4 Installation Perimeter

An installation is a defined base, camp, post, station, or other activity under the jurisdiction of the DoD, including any leased space. This security layer is usually not considered to be close to the asset and is usually not designated as the Asset Container Layer perimeter by the design team. When the access control perimeter is at this layer, personal authentication assurance commensurate with the value of the assets being protected will be required at any entrance to the installation. Figure 2-2, item 1, uses fencing to depict an example of an installation perimeter that may be used.

While control method at the installation layer can add to the defense of an asset, this is not always the case. Some commercial installations do not lend themselves to implementation of stringent installation perimeter controls. While Government-owned installations frequently implement multiple controls at this perimeter, commercially leased spaces such as office parks are generally open to the public. Many do not have a building guard or attendant and many cities or owners object to certain types of barriers and security controls.

The barrier is the primary means of access control at this layer. A barrier is an obstacle that prevents or controls movement of persons or vehicles. At the installation layer, the barrier is a physical security measure that prevents penetration of an installation. Barrier defenses are intended to be obvious to the potential intruder and are generally clearly marked with warning signs. Assessment and selection of a barrier solution must consider two potential penetration types: overt penetration by force and covert penetration by stealth tactics. The objective of a barrier is to physically or psychologically discourage a less determined attacker, delay a more determined attacker, and to channel the flow of personnel and vehicles.

All barriers can be compromised given enough time and resources. The objective when designing this layer is detection and delay of the attacker, giving responders enough time to neutralize the attacker. The security architect should consider the following: layering of barrier types; implementation of penetration detection systems such as alarms and sensors; and an incident response plan.

NOTE: Many of the same techniques can be used at either the Installation or the Building Perimeter.

This page is intentionally left blank.

3. ACCESS CONTROL METHODS

This section defines access control methods used in asset protection solutions and details the policies, which must be applied. These solutions may be implemented at any layer of the security architecture and may be combined to achieve the desired asset assurance level. Additional information on these combinations is given in a subsequent section.

Access control methods are specific physical or logical techniques that can be implemented at each security architectural layer to control and monitor access in and around the controlled area. There are three general types of access control methods: logical, physical, and administrative controls. Logical control methods are technical, employing hardware and software in various configurations and degrees of sophistication. Logical controls include smart cards, passwords, and firewalls. Physical perimeter controls form a layer of protection using interior or exterior controls to deter or delay aggressors attempting forced, visual, or electronic access. Physical controls include fencing, barriers, and guards. Administrative controls use policies and procedures and are critical to the success of physical and logical control methods.

An access control perimeter is protected by access control methods that are appropriate based on the asset's value, vulnerabilities, and environment. The technical capabilities of a logical control may be negated by the need for constant maintenance because the desired ACP is in an environment, which adversely affects the hardware of the biometric, card reader, or remote video system.

Methods are also evaluated based on effectiveness in mitigating likely attacks. The types of tactics against which protection is needed will differ for physical assets/perimeters and logical assets/perimeters. Control methods such as doors with locking mechanisms based on Personal Identification Number (PIN) entry or presentation of a memory card can be defeated given enough time, opportunity and expertise. The adversary must be physically present to gain unauthorized physical access. If an attendant or guard is used to validate a photograph or ensure proper use of biometric systems (attended access control), then this type of attack may be mitigated.

On the other hand, a successful breach of a logical access control method is not as obvious. The adversary does not have to be physically present and without the appropriate access controls, a successful breach may be difficult to discover since physical evidence is not left behind. An adversary attempting to defeat a logical data container perimeter is seeking access to data protected in an information system. In this case, an access method aimed at detecting unauthorized attacks must be integrated into the access control architecture. For this reason, use of a combination of both physical and logical controls are often employed in DoD to protect access to high value assets.

3.1 Identification Credentials

The primary function of access control is to allow authorized access and prevent unauthorized access. Credentials are used to establish the true identity of a person who is claiming the right to access a controlled area or asset. Before receiving credentials, an applicant must demonstrate that the identity claimed is real, and that he or she is the person who is entitled to use that

identity. Best security practices include processes for identity proofing and issuance of identity credentials in accordance with established DoD policies. Credentials can be either physical (e.g., photo identification) or logical (e.g., network user name and password). Once issued, the credential serves as the definitive assertion of identity but must be authenticated before the presenter is allowed final access to a protected asset.

Obtaining access to a controlled asset requires the user to present identification credentials for authentication. The individual must also have authorization to access the asset, regardless of the validity of the identity. Obtaining access to DoD assets involves several steps.

- Identity proofing, where the claimed identity of the individual is validated. In DoD, this requires background checks and other means of verifying documents, biometric comparisons to criminal history database, and other information provided by the claimant.

- Collection or generation of identity credentials using authentication factors such as PINs, Public Key Infrastructure (PKI) tokens, photographs and/or biometric reference data.

- Registration and issuance of the credential, binding the credential to an identity.

- Assessing access privileges based on validated identity and need-to-know.

- Allowing or denying access privileges based on proper use of the identity credential.

DoD Directive 8190.3, *Smart Card Technology*, mandates the use of the Common Access Card (CAC) as the "standard identification card for active duty Uniformed Services personnel (to include the Selected Reserve), DoD civilian employees, eligible contractor personnel, and eligible foreign nationals". The Directive mandates that the CAC will be the principle card used to enable physical access to buildings, installations, and controlled spaces. While the Security Manager can employ local authentication methods, the DoD Directive requires that individuals are authenticated via a CAC prior to enrollment in any local authentication scheme. The ability to authenticate one's identity to a valid CAC gives the Security Manager confidence that the cardholder is who he or she claims to be. If personnel are enrolled in legacy access control system prior to being issued a CAC, the local Security Manager shall authenticate those personnel to their CAC once they have been issued. Individuals who cannot be authenticated via the CAC shall have access privileges revoked until their identity is validated.

- *(AC31.010: CAT III) The Security Manager will ensure the CAC is used as the standard identification card for active duty military personnel, Selected Reserve, civilian employees, and eligible contractor personnel.*

- *(AC31.015: CAT I) The Security Manager will ensure all individuals are identity proofed in compliance with DoD policy prior to issuing a DoD CAC or any local identity credential.*

- *(AC31.020: CAT II) The Security Manager and IAM will ensure authorized users are trained to exercise care in the protection of their CAC or locally issued identity credential.*

- *(AC31.025: CAT III) The Security Manager will ensure the CAC is the principle card used to enable physical access to buildings, installations, and controlled spaces. If the CAC is not used, a documented migration plan for use of the CAC is required.*

- *(AC31.030: CAT III) The Security Manager will ensure the CAC is used to enable Information Technology systems and applications that access the Department's computer networks. If the CAC is not used, a documented migration plan for use of the CAC is required.*

- *(AC31.035: CAT I) The Security Manager will ensure procedures exist for revoking, reporting, and reissuing credentials in accordance with DoD policy for the DoD CAC and local identity credential.*

- *(AC31.040: CAT I) The Security Manager or IAO will ensure foreign nationals do not have unescorted access to DoD facilities or areas of DoD facilities where access is controlled unless the access is approved in compliance with DODD 5230.20, Visits, Assignments, and Exchanges of Foreign National).*

- *(AC31.045: CAT II) The Security Manager will ensure Foreign Nationals who are authorized unescorted access to DoD facilities are issued badges or passes that clearly identify them as Foreign Nationals.*

- *(AC31.050: CAT I) The Security Manager will ensure authorized personnel validate the identity of any person prior to issuing an authentication token (such as an unescorted visitor's badge, a CAC or local identity credential) to that person.*

3.2 Personal Authentication

When an individual presents an identity credential at a logical or physical access control point, the credentials must be authenticated as valid and bound to the claimant. Credentials are authenticated using one of three personal authentication factors or techniques. The three categories of authentication factors are:

- *something you know* (e.g., a password),

- *something you have* (e.g., a token or smart card), and

- *something you are* (a biometric comparison).

Single-factor authentication is defined as the use of any one of these categories or authentication factors. If two factors are employed, this is considered two-factor authentication. Finally, if all three factors are required then this constitutes use of three-factor authentication. Individual authentication assurance increases when you combine authentication technologies and techniques, especially when combining differing authentication factors.

The level of assurance provided by a personal authentication method such as a smart card, key, or token, is increased as the number and types of authentication factors are increased. The table in Section 4 will assist the security manager in choosing valid combinations, which will provide the desired level of protection based on the value of the asset being protected. The tables illustrate the aggregated protection provided by the most frequently used authentication methods and will further explain how the concept of something you have, something you know, and something you are can be leveraged to optimize the access control architecture.

HSPD12 policy will require use of the Personal Identity Verification (PIV) to access Government assets up to the FOUO level by Government employees and government contractors' employees. Because classified and mission critical assets require greater levels of authentication assurance than FOUO assets, three-factor authentication should be employed by Security Managers for protection of these assets. Because it will not be practical in the foreseeable future to ensure that every DoD computer is equipped with the required peripherals and has required network connectivity to implement three-factor authentication at the asset container layer, Security Managers will continue to leverage physical access control protection layers (as illustrated in Figure 2-1) to provide required I&A assurance to support logical access control.

- *(AC32.010: CAT I) The Security Manager will authenticate identity credentials using multi-factor authentication prior to allowing access to controlled and/or restricted areas and information.*

- *(AC32.015: CAT II) The IAM and Physical Security Manager will ensure authorized individuals are trained to validate claimed identity of potentially unauthorized individuals they encounter in controlled areas.*

- *(AC32.020: CAT I) If attended access is used or required as part of the access control solution, the Security Manager will ensure guards and other authorized personnel compare individuals they encounter with the photograph printed on the surface of the CAC or other identity credential to verify that the credential is in possession of the person to whom it was issued.*

3.3 Authorization

Authorized access to an asset or data within a controlled area or computer system requires identification and authentication of the person requesting access. Once the user is authenticated, the system must be configured to validate that the user is authorized (has a valid need-to-know) for the asset being protected and can be held accountable for any actions taken. Authorized access to logical assets can be implemented as a combination of manual, automated, and/or administrative methods. A deny-by-default policy, where access to physical or logical assets is denied unless explicitly permitted is mandated by DoD policy.

The decision to grant or deny access to an asset is the responsibility of the asset owner. Logical or physical access control lists are used to record individual rights and permissions. This list can be a physical log, which is checked by an attendant but is usually automated. Authorization is

performed at the asset container perimeter once identity and authentication procedures are completed. Criteria for assigning authorization to a protected asset, involves assessing the necessity for access to, knowledge or possession of, specific official DoD information required to carry out official duties.

- *(AC33.010: CAT II) The Security Manager or IAM will ensure users have a validated need-to-know before granting access to controlled information.*

- *(AC33.015: CAT II) The IAM will ensure:*

  - *Discretionary or role-based access controls are established and enforced using access authorization forms signed by the information owner; and*

  - *System Administrators use these forms to configure logical controls (operating system and application).*

- *(AC33.020: CAT I) The Security Manager or IAM will ensure only authorized personnel with appropriate clearances are granted physical or logical access to restricted or controlled DoD facilities and assets.*

- *(AC33.025: CAT I) The Security Manager or IAM will ensure mechanisms are in place to verify individuals are still authorized access and permissions have not been revoked.*

3.4 Logical Access Control Methods

This section discusses technologies and techniques commonly employed within DoD to support the validation of the digital identity of an individual. Historically, username and password combinations have provided identification and authentication for access to networks, clients, and automated access control systems. With the advent of new technology, additional logical access control methods provide improved assurance, particularly when combined to result in multi-factor authentication. Logical and physical control methods can be combined or interchanged to give equivalent assurance depending on the environment and technical requirements of the data owner and organization.

Although the DoD CAC is the primary device used to implement logical access control. This smart card contains and implements multiple technologies. However, other technologies are presented in this section first and will serve to explain additional methods and controls that can be used as part of an integrated solution as needed by persons responsible for integration of security solutions.

- *(AC34.010: CAT I) The IAM will ensure security services for logical assets are provided to the maximum extent possible via standard security protocols (e.g., Secure Sockets Layer, Transport Layer Security, and Secure/Multipurpose Internet Mail Extensions) and shall use algorithms and key strengths as defined in DoD X.509 certificate policy.*

3.4.1 Network Architecture Controls

DoD policy requires use of logical access control mechanisms to protect the Enclave. These mechanisms are extensively described in the Enclave and Network Infrastructure STIGS and are not repeated in this STIG. Sites implanting these network infrastructures should comply with the access control implementation policies in the appropriate STIGs. These mechanisms include:

- Remote Access Servers: A Remote Access Server (RAS) or Network Access Server (NAS) serves as the access control point to the Enclave perimeter. NAS provides all the services that are normally available to a locally connected user (e.g., file and printer sharing, database and web server access, etc.). Permission to dial into the local network is controlled by the NAS and can be granted to single users, groups, or all users. NAS and RAS devices can also interface with authentication servers.

- Authentication Servers: Remote Authentication Dial-in User Service (RADIUS) and Terminal Access Controller Access System (TACACS) provide access and authentication for remote users.

- Access control lists (ACL): Include restrictions on inbound and outbound connections, as well as connections between LAN segments internal to the site/enclave.

- Firewalls: Controls the traffic flow between a trusted network and an untrusted network. Usually firewalls are used to protect the boundaries of a network.

- Logical IDS: Network and workstation mechanisms that monitors network traffic and provide real-time alarms for network-based attacks Service Network.

- De-militarized Zones (DMZ): A perimeter network segment that enforces the internal networks information assurance policy for external information exchange.

- Audit Log and Log Analysis: Network, server, and application logging is required to protect DoD restricted information. On large networks, this service is usually centralized to a logging server although some devices or applications cannot support this capability and must log on the device. Devices without any auditing capability should not be used in the DoD Enclave. Minimum requirements for activity logs depend on the type of device or application and are available in the Network Infrastructure or applicable operating system STIGs. While logging itself is automated, log analysis can be automated and/or manual. A sound best practice, particularly for critical systems, is that someone other than the system administrator should perform log analysis. Personnel with access to system logs should be specifically designated and assigned permissions accordingly. The Security Manager, IAM, or designated personnel will review system activity logs regularly looking for trends and anomalies which can help identify configuration errors, understand past intrusions, troubleshoot service disruptions, and react to probes and scans of the network.

- *(AC34.015: CAT II) The IAO will ensure the Enclave architecture and components are in compliance with the Enclave STIG and the Network STIG.*

3.4.2 Network Port Security

Network ports should be both physically and logically secured to prevent unauthorized access to the DoD Enclave. These security measures are particularly critical when considering SIPRNet and wireless access controls. Unused ports on the network should be disabled until needed. Furthermore, if Virtual Local Area Networks (VLANs) are used on a network, a good security practice is to place disabled ports in a separate VLAN. When a computer is plugged into a network port, prior to authorizing access to logical resources, procedures should exist to: verify the computer is authorized access; verify that the user is authorized access; and verify that the computer configuration is compliant with security standards.

- *(AC34.020: CAT III) The IAO/NSO will ensure disabled ports are placed in an unused VLAN.*

- *(AC34.025: CAT I) The IAO/NSO will ensure either port security or 802.1X port authentication is used on all access ports and configured in accordance with the Network Infrastructure STIG.*

- *(AC34.030: CAT II) The IAO/NSO will ensure if Port Security is implemented, then the* MAC addresses are statically configured on all access ports.

3.4.2.1 Port Authentication

Network appliances can be used to implement electronic locking of network ports. These devices are sometimes referred to as "lockboxes". This physical security method is implemented by "locking" a port to one or more specific MAC addresses. Only these devices are allowed to access that network port or ports. If someone were to unplug the original device and attempt to accesss the locked port with a different device, they would be unable to receive any traffic from the port. This can be an important aspect of physical security for ports installed in locations such as conference rooms or other uncontrolled areas.

A network port authentication appliance can also be used to audit devices seeking access to the network for vulnerabilities and enforce customer-chosen access-compliance standards at the network switch level. But the appliance itself sits outside the direct line of traffic, using out-of-band monitoring to watch connections, so it does not drag down network performance. The appliance works without installing a monitoring agent on computers or other devices, which also helps with network performance. When a computer attempts to connect to the network without the proper security software and updates installed on the computer, it is quarantined and required to upgrade before they can connect. These devices can be configured to work with wireless, Windows, or Web-based access.

3.4.2.2 Port Authentication using 802.1X

The 802.1X protocol is an authentication standard that can be used for wired or wireless networks. This standard provides for user/device authentication as well as distribution and management of encryption keys. Individual client sessions use different keys and keys are changed dynamically.

There are three components that are used to create an authentication mechanism based on 802.1X standards: the client/supplicant, the authenticator, and the authentication server.

- Client/Supplicant: The client, or supplicant, is the device that needs authenticating to the network. It supplies the username and password information to the authenticator. The client uses the EAP to talk to the authenticator.

- Authenticator: The authenticator is the device performing the 802.1X port authentication to control access to the network. The authenticator receives the username and password information from the client, passes it onto the authentication server, and performs the necessary block or permit action based on the results from the authentication server. The authenticator uses RADIUS to speak to the authentication server.

- Authentication Server: The authentication server (e.g., RADIUS) validates the username and password information from the Client and specifies whether or not access is granted. The authentication server can also be configured to specify authorization by assigning the device or port to a VLAN access.

802.1X clients use the EAP and EAP Over LAN (EAPOL) to secure communications between the client and authenticator. Before the client is authenticated, the network port is set to the unauthorized state and only allows EAPOL authentication traffic between the client and the authentication server. All other normal data traffic is blocked. When the client authentication is complete and access is granted, the controlled port is set in the authorized state and is granted network access. To authenticate a client, the authentication proxy will compare the username and password entered by the client to the user identification and password parameters in the authentication directory (e.g., LDAP or Active Directory) to authenticate the client. Once the client/user is authenticated successfully, proper authorizations must then be associated with the user.

Wireless port access is a particularly vulnerable area where port security solutions are critical. Use of 802.1X authentication has been made mandatory by the 802.11i WLAN security standard, thus products meeting the WPAv2 requirements will be compatible with enterprise level 802.11i authentication servers, such as the Remote Access Dial-in User Service (RADIUS) server. The RADIUS server can then pass off the backend authentication to enterprise authentication services provide directory services such as Active Directory, or Lightweight Directory Access Protocol (LDAP).

The use of 802.11i configured to use AES encryption, 802.1X authentication services along with the EAP provides the best solution for the enterprise level network, particularly a high security environment. Additionally, 802.1X can be used to provide a layer of protection from unauthorized wireless access points on the wired network, as all devices are required to provide authentication credentials to the network switch port prior to obtaining access.

- *(AC34.035: CAT II) The IAO/NSO will ensure that LDAP passwords on production systems are encrypted.*

- *(AC34.040: CATII) The IAO/NSO will ensure when utilizing 802.1X, a secure EAP type (EAP-TLS, EAP-TTLS or PEAP) resides on the authentication server and within the operating system or application software on the client devices.*

- *(AC34.045: CAT I) The IAO/NSO will ensure if 802.1X Port Authentication is implemented, all access ports start in the unauthorized state.*

- *(AC34.050: CAT II) The IAO/NSO will ensure if 802.1X Port Authentication is implemented and re-authentication occurs every 60 minutes.*

3.4.3 Encryption

Encryption uses cryptographic algorithms to provide privacy and integrity when used to protect logical assets. Depending on the configuration, these techniques help protect transactions against interception and manipulation while in transit or at rest. There are two general types of encryption techniques used in DoD: secret key (symmetric) and public key (asymmetric).

Private key encryption is designed to protect information between two (or few) parties. It uses only one secret key to perform the encryption and decryption process. The single key must remain secret so the encryption will be secure since anyone with the key can decrypt the message. This presents a limitation if a private secure channel for transmitting the shared key is not possible since the key may be compromised in transit. Nonrepudiation is not possible in private key encryption schemes, since digital signatures are not supported.

On the other hand, public key encryption is designed to protect information between large numbers of people. In public key encryption schemes, each participant has two different keys (a key pair), one key for encryption (public key) and another for decryption (private key). Public keys are published openly to anyone in the network and can be sent over non-secure channels. In a public key encryption scheme, information is encrypted using the public key of the intended recipient. Only the individual with the corresponding private key can decrypt the message. Consequently, each individual protects his or her secret key, which is not meant to be shared. In DoD's public key implementation, an individual's secret keys are securely stored on the CAC, which functions as a hardware token. A passphrase or password is required to access or use the private key that is stored on the CAC. Nonrepudiation is possible in public key encryption schemes by using digital signature techniques. Requirements for public key encryption are discussed in more detail in a later section of this document.

Encryption may be used to protect the confidentiality of communications in one of two ways.

- End-to-end encryption – The data or message is encrypted from the sender to the receiver. Protocols such as Secure Multipurpose Internet Mail Extensions (S/MIME) and Secure Socket Layer (SSL) are examples of this technique. S/MIME provides end-to-end e-mail encryption when used in conjunction with DoD PKI.

- Virtual Private Networks (VPN) - A private data network that maintains confidentiality through use of encryption and security procedures across a shared public

telecommunications infrastructure. The data is transported or tunneled across a public or private network employing encryption technologies such as Internet Protocol Security (IPSec), Layer 2 Tunneling Protocol (L2TP), and Point-to Point Tunneling Protocol (PPTP). Typically, VPN encryption is implemented at the local network entry point (i.e., the firewall or Premise router), thereby freeing the end systems from having to provide the necessary encryption or communications security functions.

Encryption can also be used to protect the data stored on the hard drive of the client system. Some products, such as Microsoft's Encrypted File System (EFS), perform encryption and decryption transparently as the user stores and retrieves files unto fixed or removable storage media. This type of encryption is used to protect information on mobile devices such as laptops, which are more susceptible to theft. When using EFS, ensure that the temporary and paging files version of protected files are secured. These files should not be stored in plain text and must be removed when no longer needed.

Use of encryption is required when sensitive unclassified or classified information is transmitted over an untrusted public network domain (e.g., the Internet). Prior to purchasing new products, verify that the products are NSA approved and that they are compliant with: HSPD-12, FIPS 201, and FIPS 140-2. If used for classified systems the device used must also be Type 1 certified. A list of FIPS 140-2 products is available at the NIST website at http://csrc.nist.gov/cryptval/.

Although encryption techniques are an effective means of providing assurance of a user's identity, it does not adequately mitigate threats such as viruses and denial of service attacks. Since encryption does not ensure that only authorized individuals can access data and files, encryption must be paired with a system that defines which applications, systems, or data a user is authorized to access.

- *(AC34.055: CAT II) The IAO/NSO will ensure privileged access (i.e., administrative access) to network devices are secured using FIPS 140-2 validated encryption such as AES, 3DES, SSH, or SSL.*

- *(AC34.060: CAT II) The remote user will employ a FIPS 140-2 approved file encryption algorithm (i.e., AES, 3DES) to encrypt sensitive government files, folders and/or storage devices on remote or mobile client devices.*

- (AC34.065: CAT II) *The IAM will ensure encryption tools are FIPS 140-2 validated.*

3.4.3.1 PKI

PKI is a set of components that provide for the secure and trusted distribution of encryption and digital signature services. These services include validating digital certificates, using public key cryptography, time stamping and deploying certificate authorities that enable agencies to use PKI to manage the enterprise network security infrastructure. A cryptographic digital signature provides authentication assurance and ensures data integrity. Recipients of data that have been digitally signed by a valid system user can verify that the digital signature is valid (not been

revoked). The recipient can detect data changes caused by unauthorized modifications or corruption. Digital certificates are widely used for server authentication (site-to-site VPN gateway authentication) and strong user authentication in both wired and wireless networks (e.g., on wireless local area network using 802.1X with EAP-TLS).

Another important component of PKI is a X.509 formated certificate, a document that is signed by a trusted certificate authority (CA) and validates the originator of the public key. In order to obtain a valid certificate, the key pair owner must sign a certificate requesting permission to participate in the network and send it to the CA. The certificate request provides the CA with information about the owner of the key pair and a copy of the public key.

The DoD CAC is the hardware token entrusted to protect DoD private keys associated with identity, digital signature, and encryption certificates issued by the DoD PKI. The card enables users to access secured applications, digitally sign electronic documents and encrypt and decrypt information. The CAC contains and protects the cardholder's public and private keys and digital certificates. Under DoD's PKI implementation, a user's private key(s) are generated on the CAC and never leave the CAC. The user must provide a password or CAC PIN to invoke encryption functionality. When used to support cryptographic functions, the DoD CAC represents two-factor authentication (*something that you have* and *something that you know).*

DoD policy requires that web-based applications and computer networks use digital certificates for user authentication and that email be digitally signed. Information systems and applications other than email that incorporate the use of PKI for digital signatures must be interoperable with the DoD PKI and shall follow Department-wide interoperability guidelines for digital signature solutions. If applications are not yet PK-enabled, a DoD compliant username/password combination will be required after initially logging on to the NIPRNet using DoD PKI. SIPRNet PKI user certificates are not being issues as of the publication of this STIG but are planned for future implementation.

DoD agencies will implement DoD PKI for logon in accordance with DoD policies as follows.

- *(AC34.070: CAT II) The Security Manager will ensure certificates used for authentication are used in accordance with DODI 8520.2, PKI and Public Key (PK) Enabling, 1 April 2004.*

- *(AC34.075: CAT I) The IAM will ensure use of DoD-approved PKI digital certificates to authenticate requests for access to FOUO, Confidential, and Secret level government assets.*

- *(AC34.080: CAT II) The IAM will ensure implementation of smart card-based logon (the CAC or an equivalent assurance level DoD PKI token) to the NIPRNet using DoD PKI by July 2006, as required by DoD policy. DoD PKI will be required for SIPRNet when implemented in the future.*

- *(AC34.085: CAT I) The IAM will ensure DoD PKI is used for logon to DoD Enclaves, networks, servers, desktop, laptops, and other network capable client devices. If PKI logon cannot be used, then a DoD compliant password may be used and a migration plan implemented.*

- *(AC34.090: CAT I) The IAM will ensure PKI is required for the exchange of For Official Use Only (FOUO) information with vendors and contractors, the DoD will only accept PKI certificates obtained from a DoD-approved internal or external certificate authority.*

- *(AC34.095: CAT I)The IAM will ensure that DoD contractors who are not eligible for a DoD CAC get and use digital certificates issued by approved external PKIs when interacting with DoD PK-Enabled information systems or accessing DoD restricted information and logical assets.*

- *(AC34.100: CAT III) The IAM will ensure SAs are trained on administration and implementation of PKI and PKE. At a minimum, this training will include:*

  - *PKI awareness training*
  - *How to configure systems for CAC/PKI logon*
  - *How to configure systems for digital signature*
  - *How to configure systems for email encryption*
  - How to configure systems for Web server soft certificates

DoD PKI will be used for email and web services in accordance with the following policies.

- *(AC34.105: CAT II) The IAM will allow only certificate-based client authentication to DoD web servers using certificates issued by DoD-approved PKI certificate authorities. (This requirement does not apply to public web servers but only to web servers, which restrict access to authorized DoD personnel).*

- *(AC34.110: CAT II) The IAO will ensure Browsers, including those that support software tokens, support the use of CAC, High Assurance Remote Access (HARA) solution (as appropriate for the classification level), or NSA certified solution for storing the user's certificates, by the DoD PKI-defined deadline for migration to tokens.*

- *(AC34.115: CAT II) The IAO will ensure DoD e-mail systems shall support sending and receiving e-mail signed by DoD-approved certificates. E-mail containing DoD sensitive or restricted information, shall be signed using DoD-approved certificates. If email systems are not PK-enabled, a migration plan must be documented and emailed to ndwo@jtfgno.mil.*

Once network logon is authenticated using DoD PKI, access to applications such as databases, Commercial-off-the-Shelf (COTS), and Government-off-the-Shelf (GOTS) software applications will be PKI-enabled to the greatest extent possible. PKI authentication is not yet required but migration plans should be in place for future implementation. New COTS and GOTS application and network devise and clients must be PKI-enabled or capable. Sites should verify that products are HSPD12 and FIPS 201 compliant prior to purchase of PKI-enabled products.

Verify approval of PKI-enable products on the PKI PMO approved products list. The PIV Validation and Pre-Validation lists is located at the http://csrc.nist.gov/npivp/ web site.

- *(AC34.120: CAT II) The IAO will ensure if the application performs certificate-based authentication, then the application supports the PKI certificate class appropriate to the application's Mission Category.*

  - *Mission Categories I and II: DoD PKI Class 4 certificates, or Class 3 certificates (until the deadline for DoD PKI transition to Class 4)*

  - *Mission Category III: DoD PKI Class 3 (until DoD PKI transition to Class 4)*

- *(AC34.125: CAT II) The IAO will ensure if the application performs token-based authentication, then the application supports the type of token appropriate to the application's Mission Category.*

  - *Mission Categories I and II: CAC, or another NSA-approved Class 3 or Class 4 hardware token*

  - *Mission Category III: CAC or software token (until DoD PKI transition to CAC)*

- *(AC34.130: CAT II) If the application invokes PKI functionality to encrypt data, the IAM or responsible Security Manager will ensure the PKI function invoked by the application uses DoD PKI Class 4 or Class 3 certificates when performing the encryption.*

- *(AC34.135: CAT III) If the application performs authentication based on certificates stored in software tokens to authenticate a user in support of access control, the IAO will ensure the application is able to accommodate use of the CAC.*

- *(AC34.140: CAT II) The IAM or Security Manager shall ensure new Commercial-off-the-Shelf (COTS) software to be used in information systems that require PK-Enabling have passed interoperability testing performed by a DoD PKI Program Management Office (PMO)-approved testing facility prior to procurement.*

3.4.4 The DoD Common Access Card

Homeland Security Presidential Directive #12 (HSPD12) mandates the Personal Identity Verification (PIV) token for Federal Government employees and contractors for access to unclassified and FOUO assets. DoD plans to implement the PIV mandate by leveraging the DoD CAC, a cryptographic smart card. While any combination of PIV identity proofs could be required under varying threat conditions, three-factor authentication is not likely to be required in every case for unclassified or FOUO asset access. Implementation of the PIV may result in a number of required authentication assurance modifications to existing access control systems; however, DoD is expected to implement this mandate by July 2006 using the CAC smart card, PINs, and biometric reference data.

DODD 8190.3, *Smart Card Technology*, mandates the use of the DoD CAC as the principal identification credential within DoD. The CAC will be the principal card used to enable physical access to controlled areas and assets on the Department's computer networks. Sites are not required to discontinue use of non-CAC access control solutions; however, a migration plan showing a timeline for future compliance with DODD 8190.3 must be documented. Additional (local) credentials may be used to support access control if deemed necessary by the local Security Manager. However, in accordance with the policy, the CAC will remain the principal identification credential. Issuance of local credentials must include identity proofing using the CAC and the Defense Eligibility Enrolment Reporting System (DEERS) database. Policies for issuance of local credentials are discussed in subsequent sections.

The CAC is also the DoD PKI token. It is the authentication token required for use for access control to DoD computer networks and systems in the unclassified environment and, where authorized by governing security directives, the classified environment. PKI is a framework and infrastructure that provides services such as generation, production, distribution, control, accounting, record keeping, and destruction of public and private encryption keys used for authentication. The CAC supports PKI services including digital signature creation and validation, encryption and decryption, authentication, confidentiality, and nonrepudiation.

It is important to note that the DoD CAC is a composition of commonly used access control technologies. These technologies integrate easily into Government and Commercial-off-the-shelf products that use standard industry protocols. Integration of the DoD CAC, PKI and other technologies on the CAC should be an integral part of the access control solution to meet current and future security requirements and are mandated by government policies. The CAC can be used to support access control functions by serving as one or more of the following access control technologies.

- Identification card (photograph and text)
- Badge (worn in controlled areas)
- Memory card (data storage device)
- Smart card services (card with microprocessor)
- DoD PIV
- PKI Token
- PIN validation
- Biometric reference data storage device

Use of these authentication technologies improves security assurance and promotes interoperability across the services and throughout the Federal Government. However, there are many considerations and the policy requirements for each individual technology that affect selection and use of access control solutions and technologies. All DoD personnel and contractors listed in access control lists must be positively identified to their CAC. Applications may need to be developed or changed to make use of one or more of the enabling technologies on the CAC.

Figure 3-1 depicts the layout of the CAC and highlights the location and purpose of its components. The CAC has 32 demographic data elements stored in its integrated circuit chip

(ICC). Most of these elements are also printed on the card. The CAC has a cryptographic co-processor and secure storage to support DoD PKI function. The complexity of the microprocessor is the primary distinguishing feature between a smart card and a memory card. The CAC's barcodes and magnetic stripe store data that can be used by various DoD applications, thus, the CAC can also be used as a memory card. Most applications using the ICC will use the CAC to establish user authentication and trusted communication channels, but application data will reside in remote databases.

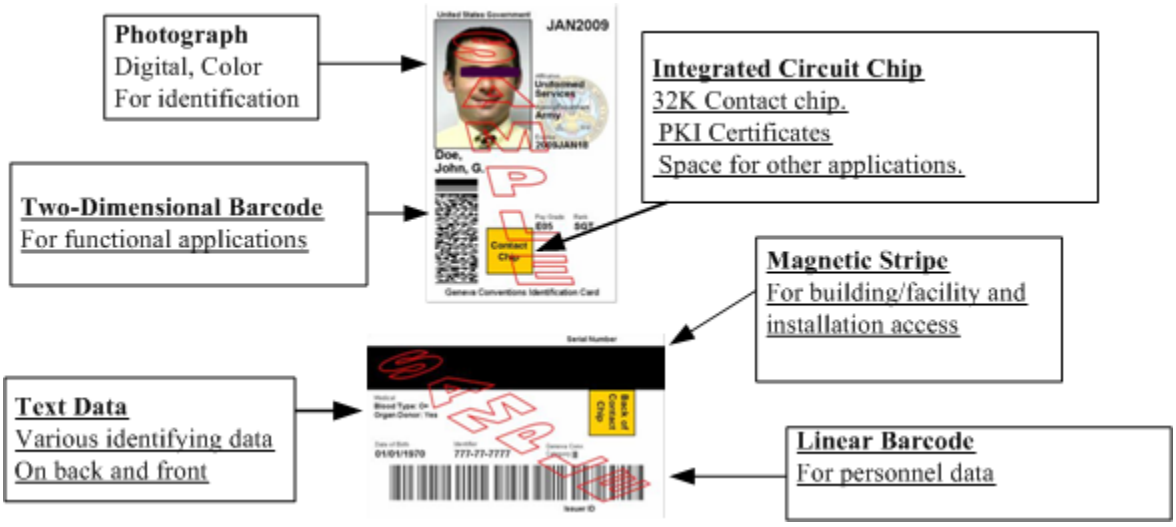

Figure 3-1. CAC Layout

NOTE: Title 18, US Code, Section 701 prohibits photographing or otherwise reproducing of departmental ID cards in an unauthorized manner. Thus, the above document is not intended to be an exact depiction of the DoD CAC.

To access the data or certificates on the chip, a PIN must be entered. The card has a routine that locks the card after four incorrect PIN attempts. To reset and re-enable the card, the cardholder must return to a CAC issuance station, present the card and proof to support validation of the cardholder's identity. Validation of the card owner's identity should include verification of his or her fingerprint against biometric reference data stored in the DEERS.

If an adversary found or stole a CAC and guessed the required PIN, he or she would have access to the digital certificates, cryptographic functionality, and other information either on the CAC ICC or accessible by use of the CAC. Certificates on CACs that are lost or stolen or on CACs held by personnel in specific personnel categories (e.g., Prisoners of War or Missing in Action) shall be revoked in accordance with DoD's certificate revocation procedure

Any application that reads and passes data to and from the CAC must be registered and digitally signed by the US Government. If the authenticated keys for this process are not present, the ICC on the card will not work and cannot be accessed.

The CAC can be used as purely an identity card, where the force protection officer or other attendant is trained to verify that the cardholder is in possession of his or her own CAC, that the

CAC is valid, and to allow or deny access in accordance with local access control policy. In an automated system, a card reader is installed at the access control point to read the stored identity information from the card's memory. The name or unique identifier is then checked in DEERS or other access control database. In each case the card is checked for expiration or revocation. This method represents single-factor authentication (*something that you have,* i.e., a CAC). Use of a memory card (*something that you have*) can only support public access of physical or logical assets, since a memory card does not meet the DoD minimum standards requiring multi-factor authentication for access to DoD protected assets.

To achieve a higher level of assurance, a keypad or keyboard can be installed at the access control point. The user presents the card to the card reader and then enters a PIN. This usage represents use of two-factor authentication or *something that you have (CAC)* and *something that you know (PIN).*

Biometric data in the form of the photograph and fingerprints are collected during the enrollment process and are stored not only in DEERS but also on the CAC. The fingerprint data is stored in encrypted form and is unlocked with the user's PIN. Using the biometric reference data stored on the ICC requires installation of a biometric reader at the access control point. Use of the fingerprint biometric comparison in combination with the CAC and the PIN, would represent use of three-factor authentication or *something that you have (CAC), something that you know (PIN),* and *something that you are (*biometric comparison).

- *(AC34.145: CAT I) The IAM will ensure access to computers and systems using PKI and the CAC are granted only when all of the following are present: the CAC, a PIN, a valid certificate, and authorization to that particular computer or system.*

- *(AC34.150: CAT II) The Security Manager will ensure the CAC is authenticated, in real time whenever possible, against the DEERS database, global directory services, or DoD PKI services.*

- *(AC34.155: CAT I) The IAM or Security Manager will ensure DoD personnel and contractors are positively authenticated before granting access to DoD protected assets or prior to issuance of any secondary authentication credential used to support access control.*

- *(AC34.160: CAT I) The Security Manager will employ the CAC as an identity credential to support access to classified assets. For access to classified assets, the CAC is combined with, at a minimum, a PIN and/or a biometric verification.*

- *(AC34.165: CAT I) The IAO will ensure the information system (network device, desktop, laptop, handheld, etc.) is configured to lock or logoff the user upon removal of the CAC.*

3.4.5 Passwords

- Passwords are still the prevalent form of authentication used for IT systems. In DoD, a password must consist of a minimum of an 8-character alphanumeric code consisting of a case-sensitive mix of numbers, special characters, and upper and lower case letters. The

system must be configured to enforce password rules and periodic checks for compliance with DODI 8500.2 (e.g., using cracking software) is required. PINS and combinations are similar to passwords and are discussed in a subsequent section. The user password represents *something that you know*.

The more difficult it is for unauthorized individuals to know, guess, or decipher the information that an authorized person knows and uses to gain access, the greater the assurance that access is controlled. Consequently, authentication methods based on *something that you know* are required to be difficult to guess and are routinely changed to make it difficult for an adversary to use a "brute force" attack to compromise the system's security. There is a trade-off between making PINs, passwords, and combinations difficult for unauthorized individuals to "crack" and making it easy for user to remember. If the authorized user has to write down the "secret" then the protected asset is vulnerable.

To protect logical assets such as computers, logon passwords and screen saver passwords must be employed. These passwords may not be written down and stored in the vicinity of the computer. The screen saver must be activated or the computer shut down if the authorized user needs to steps away. Passwords used to protect access to classified data may be written and stored in a GSA-approved container or safe and accessed prior to logging onto the computer. The password should be returned to the GSA-approved container or safe after use.

Assets stored in areas with public or heavy traffic by unauthorized individuals such as dial-up connections or entry lobbies, are at increased risk. Consequently, "secrets" that protect these assets must be diligently protected by secure PIN, password, and combination controls and procedures.

Shared passwords mean that multiple people know or share the same "secret" used to protect the assets. Nonrepudiation is not possible in systems whose assets are protected solely by shared passwords. Furthermore, when one of the members of the group of authorized users is no longer authorized (e.g.,, they retire or change jobs), the password must be changed and redistributed. Although regular password changes normally enhance security and frequent password changes may itself present more significant vulnerabilities.

To further enhance password security some organizations may use one-time password generators or hardware tokens. With this system, each user is given a password generator that looks much like a pocket calculator. To access the central system, the user enters a PIN on the password generator to gain access to it; the password generator creates a random password (or number sequence) using a procedure that is duplicated at the central system. Further discussion on these devices can be found in a later section.

Access to the NIPRNet and DoD information systems containing sensitive information will employ the DoD CAC/PKI for logon. However, some systems may not be PKI-capable. For those systems that are not PKI-capable, documentation and a migration plan is required.

- *(AC34.170: CAT II) The IAM will ensure where passwords are used for access to DoD restricted assets (i.e., networks, workstations, or applications), at a minimum, passwords are created and changed in accordance with current DoD policy. Users must be trained on this requirement and, if possible, an automated procedure must be in place to enforce these rules.*

- *(AC34.175: CAT I) The IAO will ensure default installation passwords are removed from installed devices used for production such as communications, databases, applications, or operating systems.*

- *(AC34.180: CAT II) The IAO will ensure individual users and system, application, and database administrators use their individually assigned accounts.*

- *(AC34.185: CAT II) The Security Manager and IAO will ensure shared/group PINs and passwords are used only in accordance with the DoDI 8500.2. Auditing procedures are implemented in conjunction with these methods to ensure nonrepudiation and accountability.*

3.4.6 Cryptographic or Hardware Token

Hardware tokens (also called hard tokens or eTokens) are hardware devices such as smart cards or Universal Serial Bus (USB) cryptographic tokens, usually with computing capability used to decrypt and sign in private key operations Tokens such as the DoD CAC and the RSA SecurID® are used in DoD to authenticate users at network, system, application, and desktop levels. These devices can be integrated for use with network devices such as remote access servers, wireless access points, Web servers, firewalls, and VPNs. Depending on the solution implemented, hardware cryptographic tokens, generally offer a higher level of security then passwords. Use of hardware tokens, which contain tamper protections such as zeroization of contents and tamper detection switches, is essential. When hardware tokens require the user enter a PIN, their use represents two-factor authentication, *something you have* and *something you know*. Tokens such as USB key chain tokens which generate a passcode simply by pushing a button on the device, represent single-factor autherntication, *something you have*. Tokens come in various shapes, sizes , technologies, and can perform various funtions. Some manufacturers have software implementations of the hardware tokens (commonly refered to as software tokens) and can be used with mobile devices such as PDAs. There are two general categories of tokens: identity tokens and crytographic tokens.

Identity tokens perform dynamic password and challenge/response techniques which can be used in place of traditional static, shared, or easily cracked passwords. Instead of a user being forced to remember passwords, a new complex password is automatically generated for the user for each logon or entry request. These devices perform operations to generate a code that can be used as a one-time password that can be used for network access. Some identity token devices have a keypad. System administrators may set variables such as: PIN length, complexity; entry attempts, and whether the PIN is prepended to the passcode; passcode length and complexity (numeric, alphanumeric, hexidecimal, and etc.); and the encryption algorithm used.. Use of these tokens should be limited to access control as they do not provide data, message, or network communications protection services.

Cryptographic tokens use mobile devices such as smart cards, USB key fobs, or PCMCIA cards with embedded cryptographic modules. These devices can perform more complex operations and can be used to secure or digitally sign data, messages, or network communications. The DoD CAC is the DoD approved cryptographic token and previously discussed.

Some tokens have a fixed command set and some can be programmed post installation in case of compromise or zeroization. Fixed command set cards such as the RSA SecurID token must be returned to the manufacturer to be reprogrammed. PIN, passcode, and encryption settings and managements should be configurable to meet applicable DoD requirements. One-time passwords do repeat over time so care should be given to optimizing the time before repeats occur.

One issue with procurement of hardware tokens is that protocols for this technology are not fully standardized. There are multiple protocols such as Multos, Smart Card for Windows, and proprietary protocols, which are used. Another issue is that these devices can be easily lost, stolen, or left in the computer or card reader. User training is essential to mitigate these risks.

Some DoD sites regularly use RSA SecurID tokens to support access control to logical assets with higher-level sensitivity and/or to logical assets that support critical DoD missions. The RSA SecurID is a two-factor authentication method that employs *something that you have* (the hardware token) and *something that you know* (the user PIN that must be input within a limited time window, which confounds brute force attacks). A "handshake" between the hardware token and the information system must successfully complete to enable access. DoD personnel and DoD Contractors must be authenticated via the DoD CAC prior to RSA SecurID issuance in accordance with DoD Smart Card Policy. In the event that an RSA SecurID user fails to positively authenticate to his or her CAC, the RSA SecurID® will be confiscated.

The Security Manager can use the RSA SecurID at the asset container layer for up to DoD FOUO assets, without employing other I&A at any other layer depicted in Figure 2-1. For example, to support dial up access to a DoD information network. The Security Manager can use the RSA SecurID to provide I&A assurance at the asset container layer for up to DoD Secret or Confidential assets, given that additional authentication assurance (including at least one proof of *something that you are*) is without employed at the workplace or building layer (near the protected asset) as depicted in Figure 2-1.

- *(AC34.190: CAT II) The Security Manager will ensure, at a minimum, that users are authenticated in accordance with DoD DEPSECDEF Policy to their CAC prior to issuance of a non-CAC hardware token to support access control to DoD assets. Users are trained to perform authentication of DoD personnel and DoD Contractors' personnel to their CAC.*

- *(AC34.195: CAT I) The Security Manager will confiscate any DoD issued hardware token that was issued to DoD personnel or DoD Contractors' personnel if they fail to positively authenticate to their CAC.*

- *(NET0310: CAT II) To ensure the proper authorized network administrator is the only one who can access the device, the IAO/NSO will ensure Out of Band (OOB) access enforces the following security settings:*

  - *Two-factor authentication (e.g., Secure ID, DoD PKI)*

  - *Encryption of management session (FIPS 140-2 validated encryption)*

  - *Auditing of the management session*

- *(AC34.200: CAT I) The IAO will ensure the default manufacturer password is changed for all hardware token devices used for authentication to DoD information systems.*

- *(AC34.205: CAT I) The IAO will ensure that when hardware tokens are used for authentication; the information system (network device, desktop, laptop, handheld, etc.) is configured to lock or to logoff the user upon removal of the token.*

- *(AC34.210: CAT II) The IAO will ensure users are trained on the proper handling and security procedures for DoD-issued hardware tokens, which are used to protect sensitive information access.*

3.4.7 Biometric Systems

Biometric systems are often employed within buildings to protect access to workspaces where environmental effects on performance can be optimized for sensitive electronics. The Security Manager should balance convenience to the authorized user in the conduct of his or her mission, which is to prevent unauthorized access.

Biometrics technologies compare biometric samples to formulate an opinion as to whether or not a person is known to the system. This opinion is most often rendered in a “match” or “nonmatch” decision, based on a predetermined threshold of confidence. In addition to this decision, some biometric systems return a score in addition to the decision, while others (particularly, facial recognition systems) return a rank ordered set (highest confidence to lesser confidence) of potential matches to the interrogator.

Positive biometric verification can be either a component of physical or logical access controls. Physical access refers to entry to a secure area such as a building or server room. Logical access refers to use of a computing resource such as desktop computer. The biometric hardware and software to support physical and logical access control can be and often are identical. In both cases, the biometric system captures a biometric sample from the user, compares it against a biometric reference data, and either verifies that the two are the sufficiently similar to be considered “a match” or that they are not (“non-match”). Some biometric systems are easier and more convenient to use than others, depending upon the application environment. Some biometric systems require user cooperation; others can be implemented covertly (for example, “face in the crowd” applications). Not all biometric types and applications are acceptable for use in DoD; therefore, the Security Manager should consult with resources, such as with the

Biometrics Management Office, as part of the design and selection process for biometric applications.

Biometrics technologies are *indicators* of authentication assurance with results based on a predetermined threshold with measurable (not theoretic) False Accept Rates and False Reject Rates. A biometric result should not be interpreted as proof of identity. From a security perspective, biometric verification is best deployed as a component of two-factor or three-factor authentication.

Biometric systems are fundamentally different than other types of personal authentication systems for the following reasons. It is far easier for an adversary to know a complex, machine-generated PIN that has been written down for use by an authorized user, and it is far easier for an adversary to steal or counterfeit a badge, token, or smart card, than it is for an adversary to successfully overcome a biometric system; especially when the biometric system is used in an attended access control scenario. Because of the unique skills required, fewer adversaries exist for biometric systems. However, there is still some risk. Actions must be taken to ensure the integrity of the biometric reference database and implementing attended enrollment. One shortcoming of a biometric system is that compromise of system is difficult to mitigate. Because it is easier to change a compromised password or smart card than a user's biometric, it is critical that the Security Manager ensure that extreme care is exercised when enrolling an individual in a DoD biometric system.

Users of biometric authentication systems must bear in mind a few shortcomings of this technology. A compromised password can simply be changed, however once a biometric is compromised there is no going back or changing it. For information systems that currently accept Biometrics-only for authentication, this must be combined with another authentication method such as a password in accordance with DoD PKI policy. Also, a migration plan for DoD PKI authentication must be documented.

- *(AC34.215: CAT II) The IAO and Security Manager will ensure biometric systems are implemented in accordance with the Biometric STIG.*

- *(BIO6010: CAT II) The IAO will ensure biometric technology is not the sole means of access control to sensitive or classified assets (i.e., it is one component of a two-factor or three-factor authentication solution, and that it is accompanied by a automated fallback verification system).*

- *(BIO6030: CAT II) The IAO will establish adequate alternative identification and authentication procedures for users that are unable to present the required live biometric sample. These alternative identification and authentication procedures shall be written.*

3.5 Physical Access Control Methods

Physical access control methods are commonly employed in conjunction with the logical access control methods discussed above to satisfy assurance requirements for personal authentication. Physical security measures can be active or passive and include attendant personnel, physical

barriers, electronic countermeasures, monitoring, and automated entry systems. While biometric and token readers can be integrated into information technology access control points to support two-factor or three-factor authentication, this is not always cost-effective, practical or the solution desired by the asset owner. Furthermore, DoD has a unique advantage in physical access control methods (force protection personnel) that can and should be leveraged to protect DoD assets. While the focus of this STIG is information systems, some of the assets to be protected are tangible, physical assets; for example, hard drives, backup tapes, laptops, even access to system administration consoles all need to be protected to realize access control of logical assets. The following sections address physical access control methods that pertain to logical asset protection and physical assets that are components of logical asset protection.

3.5.1 Attended Access

The entry control perimeter should be under visual control at all times during working hours to prevent entry by unauthorized personnel. This requirement may be accomplished using an attended access control method (e.g., guard or monitored video surveillance system). During non-working hours, random guard patrols throughout the facility or other safeguards that mitigate the vulnerability of unalarmed storage areas and security storage cabinets are used depending on the classification of the information being protected.

Attended access control can increase the security stance at any security perimeter layer. In many cases, manual access control methods are the critical components to access control in support of DoD missions. Attendants can be force protection officers, private security guards, or other authorized individuals assigned to monitor access control points and controlled areas. These attendants may also be authorized as trusted agents to facilitate access by emergency personnel requiring access to the controlled area after hours and/or during emergency situations. Attendants must be trained to verify identity credentials to the level of assurance required.

Attendants must have the tools necessary to complete the access control task such as authorized personnel roster; phone lists, emergency contact information, and should be able to trigger facility alarms, when necessary. For increased assurance in the workspace, authorized attendants can patrol the area or monitor remote video of vulnerable points in the perimeter.

Attended access control can be implemented as a single-factor of a multi-factor authentication solution. Examples of single-factor authentication using attended access includes: having the attendant verify the authenticity of a set of hand-carried orders or a CAC; verifying that the person requesting access knows a shared combination; or having the attendant allow only individuals that he/she personally recognizes. More importantly, attended access control enables two-factor authentication by training the attendant to take the following actions.

- Comparing a cardholder to the image printed on a badge/card (*something that you are* and *something that you have*).
- Comparing a cardholder to an image pulled from a database by use of a card, PIN, or biometric system (either *something that you are* and *something that you have* or *something that you are* and *something that you know*).

- Checking the security or anti-counterfeit features on a card presented for use (increased assurance of *something that you have*).

Using guards to oversee proper use of the personal authentication and protective barrier systems can mitigate many access control system vulnerabilities. An attendant could deter an adversary from using a lost or stolen memory card for unauthorized access. Furthermore, an adversary trying to use an artifact to spoof a biometric system could be deterred by an attendant.

- *(AC35.010: CAT II) The Security Manager will ensure that attended access control (e.g., guards and video surveillance systems are implemented in compliance with the policies of DoD 5200.1-R.*

3.5.2 PINs and Combination Codes

- PINS and combination codes are numeric or alphanumeric codes and are used with cipher locks, safes, and storage vaults. These codes are entered using a keypad or similar entry device. PINS and combinations represent use of *something that you know*.

As with the user password, the more difficult it is for unauthorized individuals to know, guess, or decipher the PIN or combination, the greater the assurance level. Consequently, authentication methods based on *something that you know* are required to be difficult to guess and are periodically changed to make it difficult for an adversary to use a "brute force" attack to compromise the system's security. There is a trade-off between making PINs, secrets, procedures, and combinations difficult for unauthorized individuals to "crack" and making it easy for user to remember. If the authorized user has to write down the "secret" then the protected asset is vulnerable.

PINs or combinations used to protect access to classified data may be written and stored in a GSA-approved container or safe and accessed prior to logging onto the computer. The documented secret should be returned to the GSA-approved container or safe after use.

Assets stored in areas with public or heavy traffic by unauthorized individuals such as building entry lobbies, are at increased risk. Consequently, "secrets" that protect these assets must be diligently protected by secure PIN and/or combination controls and procedures.

Shared PINs and safe combinations mean that multiple people know or share the same "secret" used to protect the assets or to protect access to an area wherein the protected assets are stored in the open. Nonrepudiation is not possible in systems whose assets are protected solely by shared PINs or combinations. Furthermore, when one of the members of the group of authorized users is no longer authorized (e.g., they retire or change jobs), the shared PIN or combination must be changed and redistributed. Although regular password changes normally enhance security, too frequently changing passwords may disrupt mission effectiveness or introduce system vulnerabilities.

- *(AC35.010: CAT II) The Security Manager or Network Security Officer (NSO) will ensure, at a minimum, PINs and combinations are created and changed in accordance with the DODI 8500.2. Users are trained on this requirement and, if possible, an automated procedure is in place to enforce these rules.*

- *(AC35.015: CAT I) The IAO will ensure default installation PINs or combinations are changed when installing devices used for production such as GSA-approved safes or combination locks.*

- *(AC35.020: CAT II) The Security Manager and IAO will ensure shared/group PINs and combinations are used only in accordance with the DODI 8500.2. Auditing procedures are implemented in conjunction with these methods to support accountability.*

3.5.3 Classified Storage and Handling

Protection of sensitive and classified assets must include classified storage, proper security marking, transportation, destruction, and incident handling. These requirements for access control are fully established by DoD policies and must be strictly followed because of the high value of the assets. DoD 5200.1-R provides physical protection standards for the storage of classified information. The requirements in this regulation provide the only acceptable combinations of access control methods for the protection of classified material and equipment. Director Central Intelligence Directive (DCID) 6/9 and 6/3 provides guidance for the protection of Sensitive Compartmented Information (SCI) material and equipment. Physical security requirements for SCIF areas in the Continental United States (CONUS) are also found in DoD 5205.22-M-1, DoD Sensitive Compartmented Information Administrative Security Manual.

GSA establishes and publishes minimum standards, specifications, and supply schedules for containers, vault doors, modular vaults, alarm systems, and associated security devices suitable for the storage and protection of classified information. Storage of classified material and equipment such as hard copy documents or removable hard drives must use GSA approved containers only. Containers must be equipped with a three position, changeable combination lock meeting the Federal Specification (FEDSPEC) FF-L-2740.

Physical access points to facilities housing networks and workstations that process or display classified information (Top Secret or Secret) must be guarded and/or alarmed 24 X 7 IAW 5200.1R. Intrusion alarms must be implemented and monitored with response times appropriate to the classification of the materials protected. To gain access at the access control perimeter of facilities or workplaces processing classified information, two-factor authentication is required. This requirement can be met using visual monitoring by an attendant or through use of an automated entry system (discussed in a subsequent section). Although not required for all levels of classified, either automated or manual classified access logs should also be maintained to ensure accountability. Not all classified environments include a facility layer.

All levels of classified (Top Secret, Secret, Confidential) materials must be properly marked. Transportation of classified assets must use approved and authorized couriers and/or requires use of proper cover sheets and envelops as required by DoD policy.

- *(AC35.025: CAT III) The Security Manager will ensure all physical and environmental controls are established in accordance with DODI 8500.2, DOD 5200.1R Information Security Program.*

- *(AC35.030: CAT 1) The Security Manager will ensure vaults and storage rooms for classified information meet the requirements of DOD 5200.1-R Information Security Program and DOD 5205.22-M-1, DoD Sensitive Compartmented Information Administrative Security Manual.*

- *(AC35.035: CAT III) The Security Manager will ensure controlled unclassified assets are handled, marked, stored, transmitted, or destroyed in an approved manner.*

- *(AC35.040: CAT II) The Security Manager and IAM will establish a program to recognize, investigate, and report physical and systems security incidents to include classified contamination and logical/physical penetration of controlled areas.*

- *(AC35.045: CAT II) The Security Manager and IAM will ensure network connections in areas where classified documents are processed, such as open storage areas and SCIFs, are protected to a level commensurate with the information being processed in the area.*

- *(AC35.050: CAT I) The IAO will ensure wired and wireless devices (for all classification/sensitivity level of information) are not permitted in a permanent, temporary, or mobile Sensitive Compartmented Information Facility (SCIF) unless approved by Director Central Intelligence Directive (DCID) 6/9 or 6/3.*

3.5.4 Supplemental Badges, Memory Cards, and Smart Cards

In accordance with DoD policy, the CAC is the required identification credential that will be used DoD-wide to support physical or logical access control according to DoD policy. Based on the multiple technologies on the CAC, the CAC can also be used as a DoD badge, memory card, or smart card. It is important to note that DoD policy also allows for the issuance and use of supplemental badges to accommodate special access requirements. Supplemental badges, tokens, and smart cards may be used where existing automated access control applications are not readily convertible for use with CAC technology, or when the local Security Manager determines that it is required. In the event that a supplemental badge, memory card, or smart card is issued to DoD personnel or contractors, the CAC will be used to positively identify the individual prior to issuance of a supplemental card or token. Locally issued badges and cards must be combined with other authentication methods for access to classified or sensitive areas or information.

- *(AC35.050: CAT II) When using locally issued badges, the Security Manager will comply with applicable DoD policies governing identity cards and with policies in the Identification Credentials section of this STIG.*

- *(AC35.055: CAT III) The Security Manager will submit requirements to the Access Card Office (ACO), if required, to address local mission requirements for the DoD CAC in order to minimize the total number of smart cards required by DoD personnel.*

- *(AC35.060: CAT II) The security manager will only use badges, memory cards, and smart cards to protect unclassified, non-sensitive assets. This requirement includes use of the CAC when used only as a badge without requiring authentication by PIN or biometric.*

- *(AC35.065: CAT II) The Security Manager will maintain audit logs of badge, memory card, and smart card issuance, revocation, and collection.*

3.5.4.1 Badges

Badges come in various forms and support varying levels of personalization. Personalization methods include badge-holder identifiers, including the photograph, security clearance, and signature. As badge personalization elements increase, more effort is needed to identity proof the badge before issuing. Locally produced badges must comply with DoD policy as discussed in previous sections. DoD badge types include color-coded (non-personalized) badges, enumerated badges, and personalized badges.

A color-coded badge is often used to identify visitors requiring an escort within a building or workspace. Risks are increased if authorized personnel do not strictly adhere to any required escort policy. When the CAC is used as a badge, color is used to differentiate between Government and contractor staff.

Enumerated badges are usually issued after presentation of proof of identity and verification against a list of authorized visitors. Sometimes the visitor is asked to exchange their identification credential, such as a drivers' license, for the numbered badge at the access control point. The badge is exchanged for the identification credential upon exit.

Personalized badges require an identity proofing process. These cards include verified identifying information such as the badge holder's name, photograph, and signature, which can be used to authenticate the cardholder.

Color-coded, enumerated, and personalized badges provide the Security Manager with minimal personal authentication assurance because badges are easily copied, stolen, or counterfeited using readily available technology. While the adversary needs greater skill to alter or counterfeit a personalized badge, these skills are common and the costs are low. Where increased security assurance is required, the badge should be combined with additional authentication methods as discussed in subsequent sections.

3.5.4.2 Memory Cards

Memory cards are data storage devices. These cards allow storage of information used for personal authentication, access authorization, card integrity, and applications. The card does not process information but serves as a repository of information. The data can be written to a magnetic stripe, bar code, or optically stored on the ICC. When a smart card is used as a repository of information without requiring the cardholder to input a PIN or present a biometric reference sample, the smart card is implemented as a memory card. This method is often used for "touch and go" access and does not provide high assurance since the wireless transmission can be easily intercepted. Locally produced memory cards must comply with DoD policy as discussed in previous sections.

If a user presents a memory card to a reader and enters a valid PIN using a keypad or keyboard, two-factor authentication is employed. If the access control application determines that the PIN is valid and corresponds to the memory card presented, then the user is allowed access privileges based on *something that he or she has* and *something that he or she knows*.

3.5.4.3 Smart Cards

A smart card has one or more ICCs. It can also store data using memory chips on the card. The difference between a smart card and a memory card is that the smart card processes data like a simple computer. Communication with a smart card can be via contact or contactless (proximity) interfaces. At an access control point, the smart card is presented to the reader. Many applications require the cardholder to enter a valid PIN to enable smart card and cardholder authentication and subsequent establishment of a secure communication channel between the smart card and an external application for authenticated users. This type of access represents two-factor authentication comprised of *something you have* (a smart card) and *something you know* (a PIN).

DoD is implementing smart card technology through use of the CAC, however local applications may require use of a supplemental smart card. Locally produced smart card must comply with DoD smart card policy as discussed in previous sections.

3.5.5 Protective Barriers

Barriers include concrete structures, pop-up barriers, tires, and fences. Barriers are used to channel people and vehicles to an access control point and to deter unauthorized physical access. Some barriers may have to include aesthetics because of local ordinances, which may dictate the use of heavy but attractive planters or red brick walls. Movable barriers can be stored and moved into place during high threat periods. In some instances it may be appropriate to incorporate natural barriers such as small hills, lakes and ponds, or sharp hedges. Fences can range in sophistication from simple chain link fences to chain link fences with razor wire or electric fences

The Security Manager will ensure that outdoor barriers are installed using clear zones or standoff distances on both sides of the perimeter barrier. Clear zones are to be kept free of debris and other materials.

Where possible, the government agency should control vehicle traffic to within 25 meters or 81 feet of all sides of the building. Vehicle control can involve allowing parking for vehicles of only authorized or cleared personnel. When high value protected assets are located in a commercial building with an attached parking garage, controls should be in place to monitor who and what enters and exit the garage. If knowledge of the identity of those that enter and exit the building and garage is not possible or practical, the building cannot represent the access control perimeter or be considered as part of the asset protection solution. In this case, the access control perimeter must be defined closer to the asset being protected such as the workspace or asset container layers.

Automated gates can be used to support entrances and/or exits for both vehicles and foot traffic. Readers and keypads supporting smart cards, memory cards, and PINS are often employed at both vehicle and foot traffic gates or access control points. 'Contactless' smart card devices can be issued to authorized individuals to carry in their car that function much like automated tollbooth technologies. These technologies provide a layer of security, but are vulnerable to threat or electronic interception.

Government installations need to develop access controls and a standard standoff area for installation, facilities, and buildings housing protected assets. A physical security professional will assist with decisions regarding barriers and vehicle control based on the results of the risk assessment. The primary reference for physical security policies for the DoD installation is DoD 5200.8-R. Additionally, MIL-HDBK-1013/10 contains the required design guidelines for fences, gates, barriers, and guard facilities. MIL-HDBL-1013/14 provides guidelines for the selection and application of vehicle barriers. GSA-owned buildings must comply with GSA Interagency Security Committee guidelines.

- *(AC35.070: CAT III) The Security Manager will ensure physical security access controls (including, but not limited to, installation barriers, fences, security gates, and security for windows, doors, loading docks, and garage structures) comply with GSA Interagency Security Committee (ISC) and DOD 5200.8-R guidance, depending on building ownership.*

3.5.5.1 Securing Windows, Doors, Walls

If the access control perimeter is located at the Building Layer, the Security Manager must ensure doors, windows, loading docks, garage entrances and exits, sewer and roof accesses, balconies, and fire escapes are secured appropriately. Trees, trellises or textured walls provide an adversary access to a second or third story window or balcony, and must be considered in assessing risk. Authorized individuals and users in the workspace must report broken windows, security doors, and people without required credentials encountered within controlled perimeters. Local policies and procedures must be in place to address tailgating whether the practice is allowed or not.

The surfaces of rooms, including walls, windows, ceilings, vents, and roofs are not constructed primarily as security barriers, however, they must be factored into the Security Manager and IAM access control strategy. Sound abatement between protected areas where sensitive or classified discussions take place must be considered. Sound travels effectively through ventilation shafts and can transmit through ceilings, floors, and walls. A security professional

should be employed to assist in analyzing sound abatement requirements. Unauthorized physical access through drop-down ceiling panels, attic access doors, raised floors, windows, or ventilation shafts should be obstructed. The threat of unauthorized visual access including the use of reticulating fibers or remote cameras must be considered when designing workspace protection for classified or mission critical assets. Requirements for security windows, walls, and door

3.5.6 Physical Tokens

Physical tokens consist of keys and unique documents such as DoD hand-carried orders. Access control methods used for single-factor personal authentication in DoD include simple physical keys, 3-plane (complex) keys, and hand-carried orders. These tokens are authorized for the protection of non-mission critical, unclassified, non-sensitive assets. Like PKI logical tokens, physical tokens represent *something you have.*

Simple physical keys provide minimal protection and assurance, as they are highly susceptible to copying or theft. Furthermore, the locks controlled by simple physical keys, are relatively easy to compromise. Most key systems authorized for use in government facilities, use a higher security lock and key, which is harder to manipulate and use keys that are difficult to copy. A 3-plane (complex) key is one of the more secure key systems since the keys themselves are more complicated to copy, blank key stocks are not readily available to adversaries and are more difficult to counterfeit, and the locks controlled by 3-plane keys are more difficult to compromise. Organizations must purchase keying systems from authorized GSA sources only. Key control policies and procedures, where the blanks are strictly controlled, can also mitigate this risk. Any key used is highly susceptible to theft and use by an authorized adversary.

- *(AC35.085: CAT I) The Security Manager will ensure when physical keys (regardless of type) are the only access control method used, they only allow access to unclassified, non-sensitive non-mission critical assets.*

- *(AC35.090: CAT I) The Security Manager will ensure when hand-carried documents are not to be used as a single-factor authentication method for access to sensitive or mission critical assets.*

- *(AC35.095: CAT II) The Security Manager will ensure authorized personnel validate the identity of the person presenting hand-carried documents and the documents themselves prior to granting access to DoD controlled assets or systems.*

3.5.7 Intrusion Detection Systems

Intrusion detection systems are electro-mechanical devices used at all layers of the security architecture to monitor, detect, and notify responsible personnel of physical or logical attacks. These devices include features such as remote video monitoring, alarms, motion sensors, and logging/reporting capabilities. Once notified, Network Security and Physical Security personnel must follow established response procedures as dictated by DoD policy and the specific attack underway. In addition to intrusion detection systems, exit and entrance control procedures and user training are essential to detecting unauthorized personnel in the controlled space.

Remote video enables centralized monitoring of the perimeter or controlled space. Authorized personnel can monitor the displays and alarming systems and react accordingly. Remote video can also be used where authorized individuals or pre-registered visitors present identity credentials to the reader and the attendant can remotely compare the video image and text transmitted by the smart or memory card to an authorized access control list before granting/denying access.

Intrusion detection systems can be used to detect and deter unauthorized physical access and alert guards to attempted breaches of the perimeter. Sensors can be installed at many points around and within a controlled perimeter. Environmental factors should be considered when developing the optimal strategy for any given solution. For example, motion detection sensors in areas with abundant wildlife may cause frequent false alarms and are, consequently, ineffective. Systems should be physically protected within the workspace and accessible by a few authorized personnel to ensure the integrity of these automated methods. Electrical systems supporting these devices must also be protected by an emergency back-up power plan.

Unauthorized access attempts at automated gates should alarm guards and prompt the indicated response based on threat assessment. In addition, alarms should be installed such that tampering with keypads and readers of access control systems will trigger an alarm.

3.6 Securing the Automated Entry Control System

Automated entry control systems may be used to control admittance to controlled areas in place of or as part of a multi-factor authentication solution. Protection must be established and maintained for all devices or equipment that constitute the entry control system. The enrollment stations, card readers, computer, application/database servers,, wiring, and power supplies must all be protected from tampering. These system components are as crucial to system integrity as ensuring that access control privileges are only granted to authorized personnel. Policies for securing the automated access control system are found in DOD 5200.1-R.

- *(AC36.010: CAT I) The responsible Security Manager or IAO will ensure card readers, keypads, communication or interface devices located outside the entrance to a controlled area has a tamper resistant enclosures and be securely fastened to the wall or other permanent structure. Control panels located within a controlled area require only a minimal degree of physical security protection sufficient to preclude unauthorized access to the mechanism.*

- *(AC36.020: CAT I) The responsible Security Manager or IAO will ensure keypad devices are designed or installed in such a manner that an unauthorized person in the immediate vicinity cannot observe the selection of input numbers.*

- *(AC36.030: CAT I) The responsible Security Manager or IAO will ensure systems that use transmission lines to carry access authorizations, personal identification data, or verification data between devices or equipment located outside the controlled area are protected or supervision.*

- *(AC36.040: CAT I) The responsible Security Manager or IAO will ensure access to records and information concerning encoded ID data and PINs shall be restricted. Access to identification or authorizing data, operating system software or any identifying data associated with the entry control system shall be limited to the fewest number of personnel as possible. Such data or software shall be kept secure when unattended.*

3.6.1 System Administration

Ideally, there should be a separation of duties within the administrative function of the access control system minimize the ability of a privileged user to enter false records into the system. At a minimum, the following three administrative roles should be identified and assigned:

Enrollment Administrator – the individual who verifies the identity of new users and guides them through the creation of an enrollment record.

Security Administrator – the individual who establishes and modifies the values of configuration parameters in the access control software.

Audit Administrator – the individual who reviews audit logs for security violations and related suspicious behavior.

If the access control system supports separation of duties as described above, the security administrator should activate this feature. If not, the Security Manager or IAO should implement compensating controls that make an administrator breach less likely to occur. For example, implement periodic checks to ensure that each enrolled user has an approved DD Form 2875 or similar access authorization form used to request that access. In addition, audit logs can be regularly copied to a location inaccessible to access control systems administrators so they can be reviewed independently.

- *(AC36.050: CAT II) The IAO will ensure that individuals are assigned to the following administrative roles: Enrollment Administrator, Security Administrator, and Audit Administrator.*

- *(AC36.060: CAT III) The IAO will maintain lists of individuals authorized to perform each of the following functions: enroll or re-enroll users; modify the security configuration; and review and manage audit logs.*

Preferably, the access control software will have its own administrative authentication module. If not, the systems administrator should limit permissions to all executable files to a user group whose membership consists of authorized administrators only.

- *(AC36.070: CAT II) The IAO will ensure that the following functions are restricted to authorized administrators:*

  - *Creation or modification of authentication rules*
  - *Creation, installation, modification or revocation of cryptographic keys*

- *Startup and shutdown of the access control service*

- *(AC36.080: CAT II) The IAO will ensure that only authorized Enrollment Administrators are permitted to create user access control records.*

- *(AC36.090: CAT III) The IAO will ensure that only authorized Audit Administrators can clear the audit log or modify any of its entries.*

- *AC36.100 (: CAT II) The IAO will ensure that all administrators must authenticate to the access control system to perform administrative functions and that this authentication includes a factor outside of the access control verification the system supports for ordinary users.*

Auditing for access control systems is as critical as it is for any other information system. Audit logs assist with intrusion detection as well as general troubleshooting. Investigations of information security incidents would be nearly impossible without them. It is not feasible to provide specific security guidance for audit log security given the wide variety of potential technologies involved in access control systems. Nevertheless, one can establish a relative standard that requires that audit logs be at least as secure as other logs in that environment.

- *(AC36.110: CAT II) The IAO or other responsible Security Manager will ensure that the file permissions and storage scheme for biometric audit logs is no less secure than the scheme for the system audit logs of the operating system on which the access control software resides.*

- *(AC36.120: CAT II) The System Administrator will configure the automated access control system to audit the following transactions:*

  - *All failed identification or authentication attempts*
  - *All start and stop events for the access control service*
  - *All "exact match" verification transactions for biometric systems*

- *(AC36.130: CAT III) The System Manager or responsible individual will ensure the following records are maintained IAW 5200.1-R.*

  - *Active assignment of ID badge/card, PIN, level of access, and similar system-related records.*
  - *Records concerning personnel removed from the system shall be retained for 90 days.*

  - *Records of entries shall be retained for at least 90 days or until investigations of system violations and incidents have been investigated, resolved and recorded.*

- *(AC36.140: CAT II) The Security Manager will ensure all automated access control systems are configured to use Federal Information Processing Standard (FIPS) 140-2 validated encryption algorithms for communication. Type 1 encryption is required to protect communications of classified information.*

- *(AC36.150: CAT II) The Security Manager will ensure all automated access control systems are configured to use Federal Information Processing Standard (FIPS) 140-2 validated encryption algorithms to protect data at rest.*

- *(AC32.160: CAT I) The Security Manager will ensure identification and authentication procedures are followed whenever the automated access control system is unavailable (fallback procedures must be documented).*

This page is intentionally left blank.

4. ACCESS CONTROL IMPLEMENTATION SOLUTIONS

Protection of DoD restricted and critical assets must follow a layered approach, as described in previous sections. Often, users are asked to present credentials at multiple instances as they encounter various uncontrolled and controlled areas on the way to access resources that may or may not require such protection. Under-protection of an asset may lead to compromise, however, unnecessary over-protection can be inconvenience to the users, costly, and may be detrimental to the desired security posture. Synchronizing and integrating access control mechanisms to recognize vulnerabilities is difficult and some degree of overlap in functionality must be expected. This is done by selectively aggregating access control techniques at the appropriate layer of the security architecture. The access control design or selection team should consider the following general steps when selecting personal authentication methods for the access control solution.

- Step 1: Determine the value of the asset to be protected. This assessment performed by the data owner and is based on mission criticality (MAC Level) and sensitivity level (Public, Sensitive, Classified). Determining the value of the asset being protected and the site-specific constraints are the first steps to consider when selecting access control mechanisms as part of a security solution. Value determination is done using the asset's MAC and the results obtained from a thorough risk analysis.

- Step 2: Determine the options available for use as a personal authentication strategy by consulting the personal authentication matrix located in a subsequent section. Scenarios of this process are provided in a subsequent subsection.

***NOTE*:** MAC I (critical) systems should use the matrices for classified sensitivity. MAC II and MAC III systems are not addressed specifically but users should use the matrices for the appropriate Sensitivity level.

- Step 3: Using the list of available options for protecting the asset (s), the security design team can make decisions about how the various strategies listed could be integrated into the environment based on the following variables.

    - Attended Access. Determine if attended access can or will be used as part of the access control strategy. As the matrix demonstrates, attended access can expand the number of available options significantly; therefore this condition should be integrated into the solution when possible. The security team may need to determine where to place guards and what credentials must be checked to satisfy attended access requirements of the method selected.

    - Residual risk to the Asset. This assessment is based on the results of the risk analysis and recommended mitigation or the team can recommend acceptance of the residual risk based on mission needs.

    - Environmental Considerations: Some strategies cannot be implemented because of tactical, weather, network availability, noise levels, and attendant availability or other constraints as discussed in subsequent sections. Some options consist of several

personal authentication methods (e.g. multi-factor combinations). Environmental considerations may require layering of the methods such that not all authentication proofs are used at the access control point for the asset container layer as discussed in previous sections.

- Technical Requirements: False acceptance and rejection rates, response times, maintenance, encryption, database storage, fallback, backup, frequency of access, and auditing.

- Cost: Procurement costs are impacted by availability on GSA schedule, availability of non-proprietary hardware, software and maintenance costs. Although this document does not directly discuss costs and budget for the access control system, the security selection team should bear in mind that automated solutions such as sensors, remote video, and card readers will increase the cost of the access control solution.

- Step 4: Determine the access control perimeter (outermost point in the environment that access to the asset can and should be controlled), asset container perimeter, and access control point (s). As discussed in previous sections, these may be one or more areas including the facility, building, workspace, or approved asset container. Use all information collected in previous steps to implement the access control solution. The list generated from the matrices provides the team with the minimum authentication requirements for protection at the Asset Container Layer. Selection of access control techniques and methods should be primarily based on asset value and the requirement to mitigate specific risks as determined by the risk assessment. Controls must also implement DoD policy applicable to the mission criticality and confidentiality level of the asset. The implementation may consist of a layered solution but must provide the strongest protection closest to the asset as explained in previous sections.

4.1 Assessing the Value of the Asset

The MAC level indicates the criticality of an asset to the DoD mission based on its purpose and user community. The Sensitivity level of an asset must also be determined and is based on whether the data or resource is restricted or releasable to the public. There are three MAC and three Sensitivity levels. The MAC and Sensitivity level of the asset is an important factor in determining the security strength the access control solution must provide. MAC and Sensitivity Levels are further defined in Appendix C and DODI 8500.2.

4.2 Risk Analysis

The specific access control method selected must also be based upon a risk analysis, which carefully identifies and considers the threats, risks, and costs associated with each solution. Failure to conduct a risk analysis could result in implementation of ineffective countermeasures to mitigate vulnerabilities, possibly, leading to loss of protected data, equipment, facilities, or personnel.
The risk analysis should identify potential adversaries and ways of mitigating the threat posed by likely attacks. The adversary of a physical access control system is distinctly different from the adversary of a logical access control system. An adversary attacking a physical access control

system must be physically present; therefore the risk of being caught is high. In contrast, an adversary can attack multiple logical access control systems from a remote location.

The Commander or Director will sign the risk analysis, signifying acceptance of any residual risk. The result of the analysis is normally documented in the System Security Authorization Agreement (SSAA). The analysis should be no older than the SSAA but is preferably updated annually.

- *(AC42.010: CAT III) The Security Manager will ensure a risk analysis is conducted and documented for the systems and the facility to be protected.*

- *(AC42.015: CAT III) The Security Manager will ensure unresolved or unmitigated risks (residual risks) are identified, documented, and accepted by the DAA. System changes that are needed to mitigate these residual risks must be documented.*

- *(AC42.020: CAT III) The Security Manager will ensure a security plan is prepared and signed by the commander/director or other appropriately authorized senior management official.*

4.3 Determining the Access Control and Asset Container Perimeters

A multi-disciplined team consisting of the data owner, the IAM, the organization's Physical Security Manager, and the installation, base, or building Physical Security representatives must determine this point of initial control.

Access control systems can be nested within the workspace to limit access to Government assets. For example, sensitive assets may be accessible within the entire workspace perimeter, but classified assets may be stored in a room within the workspace that only a select few are authorized to access. The concept of an internal or nested control point may serve as a perimeter for limited access and special access areas such as classified equipment in computer rooms or open storage areas where classified equipment and materials cannot be removed. The most stringent personnel authentication challenge should be located nearest the asset being protected, at the asset container layer.

- *(AC43.010: CAT I) The IAM and Security Manager will ensure open storage areas meet the requirements for open storage IAW Appendix G, DOD 5200.1-R, DOD Information Security.*

- *(AC42.015: CAT III) Once the perimeter is determined and established, the IAM and Security Manager will ensure standard Government warning signs or banner messages are displayed identifying the perimeter of each physical and logical restricted area.*

4.4 Determining Technical Requirements

Determining the technical requirements of the access control system requires careful evaluation of the technology available to implement the methods selected. Access controls may be as simple as a posted force protection officer granting or denying entry or it may be an automated system that uses authentication technology to control the locking and unlocking of a gate. In

many cases, both automated and manual systems are used, where the automated systems support those who routinely work in the protected area and the receptionist or guard supports visitor access processing. As discussed throughout this document, DoD policies for access control implementations mandate capabilities for false acceptance and rejection rates, response times, maintenance, encryption, database access, fallback, backup, and auditing capabilities.

An important consideration is whether the access control point will be attended or unattended. Attended access control implies that someone other than the individual requesting access permission is present and observing the access attempt. Attended access control will deter an adversary from tampering with the access control system hardware, mounting "brute force" PIN entry attacks, or presentation of artifacts to biometric sensors, for example. DoD has unparalleled strength in force protection and staff vigilance, which can be leveraged to lower the cost of the access control system since these individuals are usually already in place. Unattended access control scenarios may include after hours access or remote access.

Another issue is the environment at the access control point. Weather conditions can adversely affect the equipment and capabilities of reader hardware. The performance of biometric systems with optical sensors (e.g., facial or iris recognition systems and some fingerprint systems) is affected by light variance. Slotted readers used with memory and smart cards may not be well suited for maritime environments because of saline crystallization. Noisy environments on airfields, tactical environments, and lobbies will increase false rejection rates for voice recognition technology.

Network communications is key to validating digital signatures or conducting biometric comparisons where the biometric reference data is stored in an external database. In many systems, the biometric reference database must be stored at the access control point because the area is not network accessible. For standalone systems, a process for maintaining the database to update revocations and other changes must be part of the technical requirements. Technical requirements must also include the availability of compatible card or biometric readers for network and client devices. Some technologies may not work for these devices because of size or protocol issues. Whenever possible, the security design team should select hardware and software that is Underwriter's Laboratories (UL)-listed and exists on the GSA schedule. Applications and operating systems should not be proprietary and should use standard industry protocols approved for use in DoD.

Special user issues that are unique to the mission may also impact the design. These issues must be considered in the design. The security design team should include a user representative so that these considerations may be captured.

4.4.1 Remote Access

Access to classified information must employ stringent security for the communications and for the client device. Classified access will require use of a FIPS 140-2, Type 1 device. Remote administrative access requires the use of encryption to protect the communication. End-user access to non-public information should also employ encryption but this is not currently a DoD requirement. With the use of the CAC and PKI, encryption and strong authentication

mechanisms are more readily added to the remote access solution and must also be used prior to allowing the remote access.

For dial-up access, security configuration involves proper setting for encryption and authentication of the remote client prior to granting access. The network architecture and client configuration settings for a PPP network are discussed in the Secure Remote Computing and the Network Infrastructure STIGs.

- *(AC44.010: CAT I) The IAO will ensure FIPS 140-2, Type 1 encryption is used to protect remote access to classified networks.*

- *(AC44.015: CAT I) The IAO will ensure remote administration of network devices, servers, and applications are protected by FIPS 140-2 compliant encryption.*

- *(AC44.020: CAT I) Remote access to NIPRNet and SIPRNet resources must be approved by the DAA and must comply with NSA and DoD policies and guidelines.*

- *(AC44.025: CAT I) The IAO/NSO will ensure that an NSA approved remote access security solution (such as a HARA solution) is used for remote access to a classified network.*

- *(AC44.030: CAT II) The IAO will ensure that remote access configuration and user training is compliant with the Secure Remote Computing STIG.*

- *(NET1610: CAT II) For dial-up access, the IAO/NSO will ensure that CHAP with MD5 or MS-CHAP with MD4 encryption is used to authenticate the remote client.*

4.5 Integrating Access Control Methods

In most cases, leveraging authentication assurance from different authentication factors offers greater assurance than introducing multiple proofs of the same authentication factor. Verifying *something that you have* and *something that you know* offers greater authentication assurance than verifying possession of multiple things that you have. Furthermore, not all authentication factors offer equivalent authentication assurance. In general, *something that you have* offers less assurance than does *something that you know* or *something that you are*.

DoD policy mandates two- or three-factor authentication as dictated by the level of protection and restrictions required by the asset. As stated in a previous section, FOUO access to MAC II and MAC III assets requires use of no less than two-factor authentication. Classified and/or MAC I assets requires the protection of three-factor authentication. To ensure the access control solution meets these policy requirements, the security design or selection team should categorize each method planned for incorporation into the access control architecture as representing *something you have*, *something you know*, or *something you are*. Translating the personal authentication method into the factor will help in determining whether the solution truly represents two- or three-factor authentication. Using this methodology will enable the security design or selection team to see the aggregated protection result of the combined solution.

4.5.1 Combining a Card and a PIN

This combination represents *something that you have* and *something that you know*. Its use mitigates the threat of an adversary using a lost or stolen credential to gain access since access requires the individual to swipe the magnetic stripe or bar code of the security card (e.g., CAC) and enter a PIN. This combination can be used to support unattended access control.

Access to restricted DoD information systems requires a secure communications channel that is established using PKI. In this instance, the PIN is used by the system to unlock the authorized cardholder's private key stored on the CAC. Remote access to DoD information systems can use this method or use a security hardware token that requires valid PIN entry within a predetermined time window.

4.5.2 Combining a Card and Biometrics

This combination represents *something that you have* and *something that you are.* Its use mitigates the threat of an adversary using a lost or stolen credential or token but also adds assurance that the person presenting the card for use is the rightful cardholder. This combination of authentication techniques is often used to support high assurance in support of attended or unattended access.

Attended access control can be used in situations that require verification of the CAC using the user's biometric live-capture sample and comparing it to the biometric reference data stored on the CAC. Attended access control will help deter a potential adversary from presenting a fraudulent biometric to the biometric sensor and uses the attendant to verify that the cardholder resembles the photograph printed on the CAC. However, a very sophisticated adversary could produce a fraudulent smart card that verifies the adversary's biometric; consequently, using these procedures would provide equivalent protection to use of a CAC and a PIN discussed previously. The possible flaw in this method is that the verification occurs using the biometric stored on the card.

Unattended access control or higher-level assurance for attended access control can be achieved by requiring verification of the CAC using the user's biometric live-captured sample comparing it to the biometric reference data stored in DEERS database or a local access administrator's database. This verification does not use the biometric data stored on the CAC for verification.

The highest level of assurance that can be achieved using this two-factor combination requires validating the CAC using the user's biometric live-captured sample by comparing it to both locally stored (on card) and remotely stored (off card) biometric reference data.

4.5.3 Combining a PIN and Biometrics

This combination represents *something that you know* and *something that you are.* Its use mitigates the threat of an adversary using a lost or stolen credential and has the added advantage of user convenience (the user does not need to carry anything).

In this scenario the PIN is used much like a Userid. The user enters the PIN and then submits a biometric live-captured sample. The system compares the biometric sample to the biometric

reference data associated with the PIN entered (in a one-to-one biometric verification) Alternatively, the user could present a biometric sample to the sensor and the system could conduct a one-to-many biometric identification. The user would be prompted to supply a PIN known by the person that provided the biometric reference data.

NOTE: Biometric identification (one-to-many matching) can have performance implications depending on the size of the biometric database, and biometric verification (one-to-one matching) may be less expensive and provides faster response times.

4.5.4 Three-Factor Authentication

The maximum level of assurance that can be achieved at a single access control point is three-factor authentication which requires integration of techniques representing *something that you have*, *something that you know*, and *something that you are*. A CAC can be used in support of this level of assurance as follows:

- As an identity card, smart card, memory card or badge representing *something that you have*

- To authenticate an identity by comparing the cardholder to the biometric image stored on and/or in the CAC representing proof of *something the you are*

- As s*omething that you know* through use of the CAC PIN or the user's knowledge of a password or safe combination

However, using information stored on the CAC for all three-authentication factors illustrates why integration of access control methods and techniques can itself introduce vulnerabilities. When the CAC is used to provide all three personal authentication techniques, an adversary needs only a valid CAC and a careless, colluding, or coerced user to gain access. This vulnerability is especially serious if this method is used to protect the asset container as it provides the most direct access to the protected asset. Therefore, when all three authentication techniques are embodied in the CAC, this combination can only be used to protect unclassified or classified assets that are not mission critical.

To protect mission critical assets, the three authentication factors or techniques must be distributed across differing platforms. The CAC PIN can be used to point to a biometric reference image in the DEERS database and a trained force protection officer or guard should be in attendance to verify that a valid CAC user is not being forced.

4.5.5 Multiple Uses of the Same Authentication Factor

Multiple uses of the same authentication factor represents single-factor authentication regardless of how many methods of the same factor are used in the access control solution. Although this combination may not be used for access to sensitive, classified, or mission critical assets, requiring two uses of *something that you have* (for example, a CAC and a key to a desk drawer) is inherently more secure than using one method only. Requiring two passwords is more secure than requiring one. Requiring personal recognition by colleagues and biometrically verifying

your identity (two instantiations of *something that you are*) is more secure than either method alone. Use of this combination, when integrated well, can provided a challenge to the adversary by requiring multiple proofs of authentication for access and thus present multiple barriers to entry.

The least assurance is achieved when two proofs of *something that you have is* implemented. This is because an adversary may be able to steal or find a purse or a briefcase containing multiple authentication devices. Consequently, multiple instances of *something that you have* offer lesser access control assurance than do combinations using multi-factor authentication techniques.

Increased assurance is achieved by using two proofs of *something that you know*. While it may be possible to gain access to a single written password or PIN, it is less likely that more than one password or PIN will be written on a single slip of paper obtained by the adversary. It is possible that an adversary may overcome a user and force them to divulge all of the information required to compromise the security of a system, but this is no greater risk that forcing the authorized user to hand over tokens and divulge passwords or PINs. Consequently, multiple proofs of *something that you know* offer greater access control assurance than do multiple usage of *something that you have*, but equivalent access control assurance to a combination of multiple authentication techniques.

The maximum assurance that is achieved by two proofs of the same personal authentication technique would be attended use of *something that you are*. For example, personal recognition by a colleague and passing a biometric verification check can offer a high level of assurance. The highest assurance achieved with this method uses verification of a fingerprint biometric but also either a facial biometric, an iris scan, or hand geometry biometric. This is because the technology or technique required to defeat the security mechanisms of different biometric types are different and involve complex skill sets to duplicate.

4.6 Access Control Decision Matrix

The strongest security controls should be at the point closest to the asset. The access control perimeter is the outermost layer that the data owner and/or Security Manager depends on to ensure access control for the assets being protected. Persons inside the access control perimeter are known or trusted to a certain extent. For example, if the access control perimeter is defined at the building layer, only people authorized for building access should be allowed inside. Exceptions may be handled by providing authorized escorts for visitors. Note that the access control perimeter is not at the same architectural layer for all assets and may be the same as the Asset Container Perimeter. If the asset control perimeter is physically or logically far away from the asset, then controls should be only robust enough to satisfy the data owner and Security Manager since the difficulty of securing such a large space to the level required increases and the strength of the assurance might decrease.

Table 4-1 shows the most commonly used single-factor authentication methods any of which are suitable for use by the access control design team to provide the authentication assurance necessary to protect up to DoD unclassified assets. Note that personal authentication proofing can be distributed across layers depicted in Figure 2-1. This is particularly relevant when

designing authentication assurance requirements for systems protecting higher value logical assets, which often leverage both physical access control and logical access control methods across multiple boundaries.

Combinations of the methods in Table 4-1 can be used to protect higher levels of sensitivity levels. As discussed in detail throughout Sections 3 and 4, FOUO information requires two-factor authentication and classified information (and MAC I assets) requires three-factor authentication. Thus, the combination should represent the number of factors required to protect the asset based on value (MAC) and sensitivity level. Generally, some degree of redundancy is employed when personal authentication proofing is distributed. The most stringent, trusted authentication proofing should always be closest to the assets being protected.

The methods used in the table will be updated in later versions of this STIG to reflect input from the community, policy changes, and technology advancements. Sample scenarios intended to show how the table below is used to make access control decisions is included in Appendix D. The information used assumes that a risk analysis has been performed and the environment and value of the asset has been appropriately determined in compliance with DoD policy.

Personal Authentication Methods		
Method	Authentication Factor (s)	Description
Decal	*Something that you have*	Decal mounted onto a motorized vehicle.
Transponder	*Something that you have*	Transponder mounted on a motorized vehicle used for operating an automated entry point.
Badge	*Something that you have*	Not personalized (e.g., visitors badge without name/photo).
Key	*Something that you have*	Physical key of any kind.
Memory Card	*Something that you have*	Refers to memory cards without the PIN, whether personalized or not. (e.g., magnetic stripe, barcode, optical, or smart cards used as memory cards).
Smart Card	*Something that you have*	Refers to all classes of smart cards, whether personalized or not. Includes cryptographic and non-cryptographic cards. Includes all communications interface types (e.g., contact, contactless, and combi-cards).
Password	*Something that you know*	DoD compliant password or PIN.
Unshared Combination	*Something that you know*	Electronic safe, cipher lock, or PIN pad combination which allows individualized PINS or combinations.
Shared Combination	*Something that you know*	Safe, cipher lock, or PIN pad combination with shared combination.
Colleague Recognition	*Something that you are*	Personal recognition by peers and co-workers. Considered to be **attended access**. Document policy and train users.
User Recognition	*Something that you are*	**Attended access** control implementations wherein peers or security guard/personnel perform identification and authentication. Document policy and train users.
Fingerprint Identification	*Something that you are*	Fingerprint authentication, using one- to-many match against templates or images stored or images stored in a remote database. This is **not match on card**).
Fingerprint Verification	*Something that you are*	Fingerprint authentication using a one-to-one match against templates or images stored on the PIV, in DEERS,

Personal Authentication Methods		
Method	Authentication Factor (s)	Description
		or in a local database.
PKI	*Something that you have* *Something that you know*	DoD PKI only. Digital signature. Implies use with PIV PIN or other means of inputting the digital signature.
Encryption	*Something that you have* *Something that you know*	FIPS 140-2, NSA Certified Encryption module used. Does not include use of PKI.
Cryptographic Hardware Token	*Something that you have* *Something that you know*	FIPS 140-2, NSA Certified encryption module used in cryptographic hardware token (e.g., RSA SecurID®) to implement one-time passwords solution.
Photo ID	*Something that you have* *Something that you are*	Verified digital or optical photo ID. Use of approved procedures for verifying a non-CAC photo identification credential (e.g., drivers' license, personalized memory card or smart card). Can be implemented using **attended access**, where a guard verifies the validity of the credential and also matches (visually or using an automated system) that the photo matches the individual.
PIV Photo	*Something that you have* *Something that you are*	Procedure for verifying the photo on the PIV (CAC). Can be implemented using **attended access**, where a guard verifies the validity of the PIV credential and also matches (visually or using an automated system) that the photo matches the individual.
PIV	*Varies depending on features or technology is implemented.*	PIV card (DoD CAC). Implies that its presence and validity is verified by an automated system such as a swipe into a reader. The purpose is to validate that this is a valid PIV card only.
	Something that you have *Something that you know*	PIV (CAC) with PIN for after hour's entry into vacant workspace without after-hours attendant.
	Something that you have *Something that you know* *Something that you are*	**Attended** or two-person access control using a PIV (CAC) plus PIN. For sites without a 24 X 7 attendant but where access requires two-person control, for after-hours access one possible solution could be an automated entry system, which requires a swipe by CACs from two different individuals. The user must then use his PIV and PIN to gain access to the area where he/she can Logon as normal to SIPRNet.

Table 4-1. Personal Authentication Methods

APPENDIX A. RELATED PUBLICATIONS

Applicable Policies and Guidelines

Homeland Security Presidential Directive 12 (HSPD 12), Subject: Policy for a Common Identification Standard for Federal Employees and Contractors, August 2005.

Office of the Secretary of Defense Memorandum, "Common Access Card (CAC) January 2001.

NIST Federal Information Processing Standards (FIPS 201: Personal Identity Verification (PIV) of Federal Employees and Contractors, February 25, 2005.

DOD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program, 19 July 2004.

DOD Directive 8500.1, Information Assurance, 24 October 2002.

DOD Directive 8190.3 "Smart Card Technology," 31 August 2002.

DOD Directive 5200.1-R, Information Security Program, January 1997.

DOD Directive 5200.8-R, Physical Security Program, May 1991.

DOD Directive 5230.20, Visits and Assignment of Foreign Representatives, August 12, 1998.

DOD Directive 5230.11, Disclosure of Classified Military Information to Foreign Governments and International Organizations, June 16, 1992.

DOD Instruction 8500.2, Information Assurance (IA) Implementation, 6 February 2003.

DOD Instruction 8520.2, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, 01 April 2004.

Global Network Defense Warning Order (Warnord) 06-16 Specified Tasks For Phase 1 Of The Accelerated Public Key Infrastructure (PKI) Implementation, March 2006.

NSA Guide to the Secure Configuration and Administration of Oracle9i Database Server, 02 October 2003.

NSA Guide to Secure Configuration and Administration of Microsoft SQL Server 2000, 02 October 2003.

NIST Special Publication 800-63, Electronic Authentication Guideline.

NIST Special Publication 800-76, Biometric Specification for Personal Identity Verification, February 1, 2006.

DCID 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs), November 2002.

DCID 6/3, Protecting Sensitive Compartmented Information within Information Systems, May 2000.

DISA, Enclave Security Technical Implementation Guide.

DISA, Network Infrastructure Security Technical Implementation Guide.

DISA, Windows NT/2000/XP Addendum.

DISA, UNIX Security Technical Implementation Guide.

DISA, OS/390 Security Technical Implementation Guide.

DISA, Web Server Security Technical Implementation Guide.

Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems, Version 2.2, July 30, 2004.

General Information Sites

http://iase.disa.mil	DISA IASE site
http://www.globalsecurity.org/military/library/ policy/army/fm/	Army Field manual
http://csrc.nist.gov/cryptval/	FIPS 140-2 Products lists
http://csrc.nist.gov/npivp/	PIV Validation lists

APPENDIX B. IAVM COMPLIANCE

IAVM Related Notices

No notices at this time.

This page is intentionally left blank.

APPENDIX C. MISSION ASSURANCE CATEGORIES AND SENSITIVITY LEVELS

Mission Assurance Categories

Mission Assurance Categories (MAC) express the mission criticality and associated characteristics of the application, based on its purpose and user community. DOD has defined three MACs for use in characterization of DoD systems and applications. The application's MAC is a critical factor in determining the strength of the security mechanisms the application must provide. Table C-1 presents the mission assurance categories as defined in DODD 8500.2.

Category	Characteristics of Data	Characteristics of Systems
I	1. Vital to operational readiness or mission effectiveness of deployed and contingency forces. 2. Absolutely accurate, timely, available on demand. 3. Classified, sensitive, or unclassified.	National Security Systems (as per Clinger/Cohen Act, Title 10 of the U.S. Code, Section 2.3.10), including systems used to directly perform: - Intelligence activities, - Crypto logic activities related to national security - Command and control of military forces integral to weapon or weapons system - Other system directly critical to military or intelligence missions.
II	1. Important to support of deployed and contingency forces. 2. Absolutely accurate. 3. Can sustain minimal delay without serious effect on operational readiness or mission effectiveness. 4. May be classified but is most likely FOUO or unclassified.	Identified by combatant commands: systems that, if not functional, would preclude the performance of the mission across all operations, including the following. - Readiness - Transport - Sustainment - Modernization - Surveillance/reconnaissance - Finance/contracting - Security - Safety - Health - Information warfare - Information security.
III	1. Necessary to conduct day-to-day business. 2. No material short-term effect on support to deployed/contingency forces. 3. May be classified but is most likely FOUO or unclassified.	Required to perform department-level and component-level core functions.

Table C-1. Mission Assurance Categories

Sensitivity Levels

In addition to its MAC, another factor in determining an application's security requirements is the sensitivity of the data the application will handle. In DoD, applications handle data of three general hierarchical sensitivity levels, with additional gradations/sublevels possible within these sensitivity levels as specified in DOD 5200.1-R.

- Classified*:* DoD classifications are Confidential, Secret, Top Secret, and Top Secret /Sensitive Compartmented Information *(*TS/SCI*)*. This data, IA or IA-enable system has been determined, based on appropriate guidance, to require protection against unauthorized disclosure to prevent damage to the national security. Classified data, systems, or applications are highly sensitive and are protected at the most restrictive level of access.

- For Official Use Only (FOUO): This designation is applied to unclassified information that is exempt from mandatory release to the public under the Freedom of Information Act (FOIA). The FOIA specifies nine exemptions that may qualify certain information to be withheld from release to the public if, by its disclosure, a foreseeable harm would occur. This data, IA or IA-enable system has been determined, based on appropriate guidance, to require protection (although less restrictive than classified) against unauthorized disclosure.

- Sensitive-But-Unclassified *(SBU):* SBU is Department of State (DOS) original caveat and only they can apply this marking. This caveat should appear in DoD text only when Department of State text is used to support a DoD document. All information that is not intended for public release and is exempt from mandatory public disclosure under the Freedom of Information Act. SBU data and the systems/applications that process SBU data, is protected at the next most restrictive level of access. SBU is afforded the same level of protection as FOUO.

- Public-Releasable*:* Information with release and access that is unrestricted in terms of its confidentiality (although it may have restrictions imposed by the need for information integrity and/or availability). Public-releasable data (and the systems/applications that process public-releasable data) is protected at the least restrictive level of access. Public-releasable data includes Open access and Public access information. Public access would apply to DoD public Web pages that could be read by anyone without first presenting any credentials. By contrast, OPEN access would apply to those Web pages and other resources that require the user to first obtain and present a DoD or acceptable commercial digital certificate, with this certificate being issued to the user's browser.

APPENDIX D. EXAMPLE ACCESS CONTROL SOLUTION SCENARIOS

D.1 Example Scenario 1

- Asset Value: FOUO documents and computer connections.

- Environment: Asset location is a suite of rooms on the fourth floor of a commercially owned building in a downtown metropolitan area. The building is surrounded by other commercial buildings and does not have a parking garage. Assets are located in an open storage area.

- Analysis for determining the Access Control Perimeter: The building is commercially owned. Although there is a guard in the front entry lobby area, the guard works for the building management and there are other tenants in the building. The building entry cannot be secured and thus cannot be used as the access control perimeter. The elevator exit is similarly not within the span of control. Although the organization is the sole occupant of the floor, not everyone getting off the elevator has authorized access to the FOUO asset. Thus, the security design team must either provide a Workplace perimeter or an Asset Container Layer. A Workplace perimeter could be constructed by providing a secured (and perhaps monitored) door to the Workplace from the elevator foyer or hall and securing egress from exit stairwells, for example. If the security design team cannot establish a Workplace perimeter, the security team should assume an open storage environment.

- Solution Selection: DoD policy requires two-factor authentication for access to FOUO. Once the security design team determines the security perimeter, they consult Table 4-1. The team must determine whether or not an ACP will be constructed at the entrance to the suite on the 4th floor. If a guard or receptionist can be positioned at the ACP, the team may consider a control method, which maximizes the use of the attendant. If no guard or receptionist can be positioned at the ACP or if no ACP can be established, the team must achieve the required two-factor authentication using automated methods. Note that the guard or receptionist must be in place whenever it is possible to access the suite to employ attended access. If a receptionist only works from 9:00am to 5:00pm Monday through Friday, and access is possible after hours, the team must ensure that two-factor authentication must be implemented using another method for after hours access. Since not all authentication methods are equally high in assurance, the team can, use redundant authentication assurance methods at various system layers to increase assurance.

D.2 Example Scenario 2

This scenario is the same as for Example Scenario 1, except not all employees are authorized access to the FOUO asset. All employees need to access the suite since they need to do work at their desks.

- Asset Value: FOUO documents and computer connections.

- Environment: Asset location is a suite of rooms on the fourth floor of a commercially owned building in a downtown metropolitan area. The building is surrounded by other commercial buildings and does not have a parking garage. not all employees are authorized access to the FOUO asset. All employees need to access the suite, but some only process unclassified, non-sensitive information.

- Analysis for determining the Access Control Perimeter: In this case, the Access Control Perimeter can still be the suite door. This is the first point at which the Security Manager can exercise span of control. However, because not everyone has an equal access-level to the controlled assets, the outermost perimeter cannot also serve as the Asset Container Layer. The security design team should determine whether to secure a room within the suite to contain the protected assets and/or use a container for FOUO storage. Authentication can be distributed from the perimeter to the Asset Container Layer with the most stringent authentication closest to the protected assets.

- Solution Selection: Consult Table 4-1 for potential solutions. Since the common areas do not process sensitive information, the outermost perimeter can be controlled using a single-factor authentication. Assume that the design team decides not to use attended access. An interior office will be used for housing or storing the FOUO assets. The security team may decide to install a PIV (contactless smart card) reader at the ACP to the 4th floor suite and either a finger biometric reader or a PIN pad on the door to the inner office. All authorized occupants of the suite would be issued a PIV that is recognized by the contactless smart card reader to gain access to the suite but only the individuals authorized access to the FOUO asset would be enrolled in the finger biometric system or would be issued a shared PIN to the cipher lock.

D.3 Example Scenario 3

- Asset Value: Sensitive FOUO logical assets on a computer network.

- Environment: Assets are stored on a DoD network that is accessible from laptops connecting remotely using dialup connections to the network.

- Analysis for determining the Access Control Perimeter: Dialup connections cannot leverage physical security methods for authentication assurance. Consequently, only those authentication methods in Table 4-1 that can be implemented in unattended scenarios can be considered viable options by the security design team.

- Solution Selection: Of the options given in Table 4-1, use of either a PIV (with a PIN) or an RSA SecurID® Token (with a PIN) will be required to gain dialup access to DoD FOUO assets.

This page is intentionally left blank.

APPENDIX E. LIST OF ACRONYMS

Acronym	Definition
ACO	Access Card Office
ACP	Access Control Point
BSP	Biometric Service Provider
CA	Certificate Authority
CAC	Common Access Card
CIO	Chief Information Officer
CONOPS	Concept of Operations
CONUS	Continental United States
COTR	Contracting Officer Technical Representative
COTS	Commercial Off-The-Shelf
DEERS	Defense Enrollment Eligibility Reporting System
DEPSECDEF	Deputy Secretary of Defense
DCID	Director Central Intelligence Directive
DISA	Defense Information Systems Agency
DMDC	Defense Manpower Data Center
DMZ	De-militarized Zones
DoD	Department of Defense
DOS	Department of State
EAP	Extensible Authentication Protocol
FIPS	Federal Information Processing Standards
FEDSPEC	Federal Specification
FOUO	For Official Use Only
FSO	Field Security Operations
GSA	Government Services Agency
HSPD12	Homeland Security Presidential Directive #12
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officers
IASE	Information Assurance Support Environment
ICC	Integrated Circuit Chip
ID	Identification
IDS	Logical Intrusion Detection Systems
ISC	Interagency Security Committee
IPSec	Internet Protocol Security
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSO	Network Security Officer
OS	Operating System
OSD	Office of Secretary of Defense

Acronym	Definition
PEAP	Protected Extensible Authentication Protocol
PIN	Personal Identification Number
PIP	Post Issuance Portal
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PMO	Program/Project Management Office
PPTP	Point-to-Point Tunneling Protocol
RADIUS	Remote Authentication Dial-in User Service
RAPIDS	Real-Time Automated Personnel Identification System
SA	System Administrator
SBU	Sensitive But Unclassified
SM	Security Manager
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SDID	Short Description Identifier
SIPRNet	Secret Internet Protocol Router Network
SSAA	System Security Authorization Agreement
STIG	Security Technical Implementation Guide
NIPRNet	Non-classified (but Sensitive) Internet Protocol
TACACS	Terminal Access Controller Access System
VLAN	Virtual Local Area Networks
VPN	Virtual Private Networks